LEH908A	LEH1008A	LEH1104A-2GSFP	LEH1208A
LEH906A-2MMSC	LEH1008A-2MMSC	LEH1104A-2SFP	LEH1208A-2GMMSC
LEH906A-2MMST	LEH1008A-2MMST	LEH1104A-4MMSC	LEH1216A
LEH906A-2GSFP	LEH1008A-2SFP	LEH1104A-4MMST	LEH1216A-2GMMSC
LEH906A-2SFP	LEH1008A-2GSFP		

Hardened Managed Ethernet Switches

Use this switch in harsh environments constrained by space.

Choose from standard, PoE, and PoE+ models.

BLACK BOX
www.blackbox.com
Power 3
Power 2
Power 1
LINK/ACT
1
2
3
4
5
6
7
8
100

Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Disclaimer:

Black Box Network Services shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Network Services may revise this document at any time without notice.

We're here to help! If you have any questions about your application
or our products, contact Black Box Tech Support at **724-746-5500**
or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 60 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad
(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    A: El cable de poder o el contacto ha sido dañado; u
    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    C: El aparato ha sido expuesto a la lluvia; o
    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Table of Contents

1. Specifications 7

2. Overview 10
    2.1 Introduction 10
    2.2 Features 12
        2.2.1 Features Common to LEH900, LEH1000, LEH1100, and LEH1200 Series Switches 12
        2.2.2 LEH900 Series Also Has… 13
        2.2.3 LEH1000 Series Also Has 13
        2.2.4 LEH1100 Series Also Has 14
        2.2.5 LEH1200 Series Also Has 14
    2.3 What's Included 14
    2.4 Hardware Description 15
        2.4.1 LEH900 Series 15
        2.4.2 LEH1000 Series 16
        2.4.3 LEH1100 Series 17
        2.4.4 LEH1200 Series 18
        2.4.5 Indicators on the LEH900, LEH1000, LEH1100, and LEH1200 Series Switches 19

3. Installation 20
    3.1 Selecting a Site for the Switch 20
    3.2 Connecting to Power 20
        3.2.1 12-VDC Jack 20
        3.2.2 Redundant DC Terminal Block Power Inputs 20
        3.2.3 Alarms for Power Failure 21
    3.3 Connecting to Your Network 22
        3.3.1 Cable Type and Length 22
        3.3.2 Cabling 22

4. Switch Management 23
    4.1 Management Access Overview 23
    4.2 Administration Console (CLI) 23
        4.2.1 Direct Access 23
        4.2.2 Modem Access 24
    4.3 Web Management 24
    4.4 SNMP-Based Network Management 24
    4.5 Protocols 24
    4.6 Management Architecture 24

5. SNMP and RMON Management 25
    5.1 Overview 25
    5.2 SNMP Agent and MIB-2 (RFC 1213) 25
    5.3 RMON MIB (RFC 2819) and Bridge MIB (RFC 1493) 25
    5.4 RMON Groups Supported 25
    5.5 Bridge Groups Supported 26

6. Web-Based Browser Management 27
    6.1 Logging on to the Switch 27
    6.2 Understanding the Browser Interface 28
    6.3 System 29
    6.4 Diagnostics 37
    6.5 Port 41

6.6 Switching....45
6.7 Trunking....52
6.8 STP/Ring....54
6.9 VLAN....65
6.10 QoS....70
6.11 SNMP....73
6.12 802.1x....77
6.13 LLDP....80
6.14 Other Protocols....83

7. Command-Line Console Management....90
7.1 Administration Console....90
7.1.1 Exec Mode (View Mode)....90
7.1.2 Privileged Exec Mode (Enable Mode)....94
7.1.3 Configure Mode (Configure Terminal Mode)....97
7.2 System....100
7.3 Diagnostics....109
7.4 Port....113
7.5 Switching....120
7.6 Trunking....133
7.7 STP/Ring....137
7.8 VLAN....156
7.9 QoS....162
7.10 SNMP....165
7.11 802.1x....173
7.12 LLDP....178
7.13 Other Protocols....183

Appendix A. DB9 DCE Pin Assignment....202

Appendix B. Time Zones....203

1. Specifications

Technical Specifications

Standards	LEH900, LEH1200 Series: IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-T, 100BASE-FX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-SX/LX, IEEE 802.3x, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1W, IEEE 802.1x; LEH1000 Series also has: IEEE 802.3af; LEH1100 Series also has: IEEE 802.3at
Forwarding and Filtering Rate	14,880 pps for 10 Mbps, 148,810 pps for 100 Mbps, 1,488,810 pps for 1000 Mbps
Packet Buffer Memory	2 Mbits
Address Table Size	8192 MAC addresses
Management	RS-232 console (DB9), Telnet, SNMP V1, V2, and V3, RMON, Web browser, and TFTP management
Other	• Supports alpha ring and RSTP/MSTP/STP for Ethernet redundancy. • IP Multicast Filtering through IGMP Snooping V1, V2, and V3. • Supports port-based VLAN and IEEE 802.1Q VLAN Tagging and GVRP. • IEEE 802.1p QoS with four priority queues. • MAC-based trunking and LACP. • IEEE 802.1x Security. • Bandwidth Rate Control. • Per-port programmable MAC address locking. • Up to 24 Static Secure MAC addresses per port. • Port mirroring. • NTP synchronization. • DHCP Client/Server. • Auto-MDI/MDI-X. • Full wire-speed forwarding rate.
Connectors	LEH908A: (8) RJ-45 10/100; LEH906A-2MMSC: (6) RJ-45 10/100, (2) 100BFX MM SC; LEH906A-2MMST: (6) RJ-45 10/100, (2) 100BFX MM ST; LEH906A-2GSFP: (6) RJ-45 10/100, (2) GE SFP; LEH906A-2SFP: (6) RJ-45 10/100, (2) 10/100 SFP; LEH1008A: (8) RJ-45 10/100 PoE (802.3af); LEH1008A-2GSFP: (8) RJ-45 10/100 PoE (802.3af), (2) GE SFP; LEH1008A-2MMSC: (8) RJ-45 10/100 PoE (802.3af), (2) SC 100BFX; LEH1008A-2MMST: (8) RJ-45 10/100 PoE (802.3af), (2) ST 100BFX; LEH1008A-2SFP: (8) RJ-45 10/100 PoE (802.3af), (2)100BFX SFP; LEH1104A-2GSFP: (4) RJ-45 10/100 PoE+ (802.3at), (2) GE SFP; LEH1104A-4MMSC: (4) RJ-45 10/100 PoE+ (802.3at), (4) 100BFX SC; LEH1104A-4MMST: (4) RJ-45 10/100 PoE+ (802.3at), (4) 100BFX ST; LEH1104A-2SFP: (4) RJ-45 10/100 PoE+ (802.3at), (2) 100BFX SFP; LEH1208A: (8) RJ-45 10/100; LEH1208A-2GMMSC: (8) RJ-45, (2) GE MMSC; LEH1216A: (16) RJ-45 10/100; LEH1216A-2GMMSC: (16) RJ-45 10/100, (2) GE MMSC

Technical Specifications (Continued)

Indicators	Per unit: (3) Power Status LEDs: Power 1, Power 2, Power 3; Per port: 10/100TX, 100FX: LINK/ACT, 10/100/1000TX, 1000SX/LX/1000SX/SFP: LINK/ACT, Speed
Power	Power input: LEH900 Series, LEH1200 Series: Redundant power inputs: Terminal block: 12 to 48 VDC; DC jack: 12 VDC; LEH1000, LEH1100 Series: Redundant power inputs: Terminal block: 47 to 57 VDC; DC jack: 47 to 57 VDC; LEH900 series also has: Power consumption: 11 W max. at 12 VDC, 0.46 A at 24 VDC; LEH1000 series also has: Power consumption: Device 15 W max. (without PoE), PoE power budget: 181.6 W max., PoE power output: Ports 1–8: IEEE 802.3af: Up to 15 W/port, 47–57 VDC; LEH1100 Series also has: Power consumption: Device 15 W max. (without PoE), PoE power budget: 181.6 W max., PoE power output: Ports 1–4: IEEE 802.3at: Up to 30 W/port, 50–57 VDC *NOTE: All models support overload current protection and reverse polarity protection.*
Environmental	Temperature Tolerance: Operating: -40 to +167° F (-40 to +75° C); Storage: -40 to +185° F (-40 to +85° C); *NOTE: The switch is tested for functional operation at -40 to +185° F (-40 to +85° C).* Humidity: 5 to 95%, noncondensing
Dimensions	5.71"H x 2.36"W x 4.92"D (14.5 x 6 x 12.5 cm)
Weight	2.42 lb. (1.1 kg)

Technical Specifications (Continued)

Approvals	Standards: IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-T, 100BASE-FX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-SX/LX; Safety: UL508; UL160H (ISA 12.1201) Compliance: EMI: FCC Part 15, Class A EN61000-6-4, EN55022, EN61000-3-2, EN61000-3-3, EMS: EN61000-4-2 (ESD standard), EN61000-4-3 (Radiated RFI standards), EN61000-4-4 (Burst standards), EN61000-4-5 (Surge standards), EN61000-4-6 (Induced RFI standards), EN61000-4-8 (Magnetic field standards), EN61000-6-2; Environmental Test Compliance: IEC60068-2-6 Fc (Vibration resistance), IEC60068-2-27 Ea (Shock), Federal Standard 101C Method 5007.1 (Free fall); Environmental Requirements: Railway applications: EN50121-4, Traffic control equipment: NEMA TS1/2 ***NOTE: LEH1200 Series switches are Class 1 Div. 2 ISA 12.12.01 certified for use in hazardous environments.***

2. Overview

2.1 Introduction

The Hardened Managed Ethernet switches are available in three types: without PoE or PoE+ (LEH900 series), with PoE (LEH1000 series), or with PoE+ (LEH1100 series).

Table 2-1. Avaiilable models.

Part Number	Product Name	Description
LEH900 Series		
LEH908A	8-Port 10/100 Hardened Managed Ethernet Switch	8 ports 10/100, DC power
LEH906A-2MMSC	6-Port 10/100 2-Port 100-Mbps MMSC Hardened Managed Ethernet Switch	6 ports 10/100, 2 ports 100BFX MM SC, DC power
LEH906A-2MMST	6-Port 10/100 2-Port 100-Mbps MMST Hardened Managed Ethernet Switch	6 ports 10/100, 2 ports 100BFX MM ST, DC power
LEH906A-2GSFP	6-Port 10/100 2-Port GE SFP Hardened Managed Ethernet Switch	6 ports 10/100, 2 ports GE SFP, DC power
LEH906A-2SFP	6-Port 10/100 2-Port 100-Mbps SFP Hardened Managed Ethernet Switch	6 ports 10/100, 2 ports 100BFX, SFP, DC power
LEH1000 Series		
LEH1008A	8-Port 10/100 Mbps PoE Hardened Managed Ethernet Switch	8 ports, 10/100 PoE (802.af), DC power
LEH1008A-2GSFP	8-Port 10/100 Mbps PoE 2-Port GE SFP Hardened Managed Ethernet Switch	8 ports, 10/100 PoE (802.af), 2 ports GE SFP, DC power
LEH1008A-2MMSC	8-Port 10/100 Mbps PoE 2-Port 100-Mbps MMSC Hardened Managed Ethernet Switch	8 ports, 10/100 PoE (802.af), 2 ports 100BFX, SC, DC power
LEH1008A-2MMST	8-Port 10/100 Mbps PoE 2-Port 100-Mbps MMST Hardened Managed Ethernet Switch	8 ports, 10/100 PoE (802.af), 2 ports 100BFX, ST, DC power
LEH1008A-2SFP	8-Port 10/100 Mbps PoE 2-Port SFP 100-Mbps Hardened Managed Ethernet Switch	8 ports, 10/100 PoE (802.af), 2 ports 100BFX SFP, DC power
LEH1100 Series		
LEH1104A-2GSFP	4-Port 10/100 Mbps PoE+ 2-Port GE SFP Hardened Managed Ethernet Switch	4 ports 10/100 PoE+, 2 ports GE SFP, DC power
LEH1104A-4MMSC	4-Port 10/100 Mbps PoE+ 4-Port 100-Mbps MMSC Hardened Managed Ethernet Switch	4 ports 10/100 PoE+, 4 ports 100BFX, SC, DC power
LEH1104A-4MMST	4-Port 10/100 Mbps PoE+ 4-Port 100-Mbps MMST Hardened Managed Ethernet Switch	4 ports 10/100 PoE+, 4 ports 100BFX, ST, DC power
LEH1104A-2SFP	4-Port 10/100 Mbps PoE+ 2-Port 100-Mbps SFP Hardened Managed Ethernet Switch	4 ports 10/100 PoE+, 4 ports 100BFX, SFP, DC power

Table 2-1 (continued). Available models.

Part Number	Product Name	Description
LEH1200 Series (Class 1 Div. 2 ISA 12.12.01 certified for use in hazardous environments)		
LEH1208A	8-Port 10/100 Mbps Hardened Managed Ethernet Switch	8 ports 10/100, DC power
LEH1208A-2GMMSC	8-Port 10/100 Mbps with 2-Port GE MMSC Hardened Managed Ethernet Switch	8 ports 10/100, 2-Port GE, DC power
LEH1216A	16-Port 10/100 Mbps Hardened Managed Ethernet Switch	16 ports 10/100, DC power
LEH1216A-2GMMSC	16-Port 10/100 Mbps with 2-Port GE MMSC Hardened Managed Ethernet Switch	16 ports 10/100, 2-Port GE, DC power

2.2 Features

2.2.1 Features Common to LEH900 Series, LEH1000 Series, LEH1100 Series, and LEH1200 Series

- Meets NEMA TS1/TS2 Environmental requirements such as temperature, shock, and vibration for traffic control equipment.
- Meets EN61000-6-2 & EN61000-6-4 EMC Generic Standard Immunity for industrial environment.
- Supports Command-Line Interface in RS-232 console.
- 100BASE-FX: Multimode SC or ST type; Single-mode SC or ST type. 100BASE-BX: WDM single-mode SC type.
- 1000BASE-SX/LX: Multimode or single-mode SC type. 1000BASE-BX: WDM single-mode SC type.
- Supports 8192 MAC addresses. Provides 2 Mbits memory buffer.
- Alarms for power and port link failure by relay output.
- Supports DIN-rail or panel mounting installation.
- Power Supply: Redundant DC terminal block power inputs or 12-VDC DC jack, 100–240 VAC external power supply.

Management Support

VLAN:

- Port-based VLAN
- IEEE 802.1Q tagged VLAN

Trunking:

- MAC-based trunking with automatic link fail-over

Port Security:

- Per-port programmable MAC address locking
- Up to 24 Static Secure MAC addresses per port
- IEEE 802.1x Port-based Network Access Control

Port mirroring:

- QOS (IEEE802.1p Quality of Service)
- 4 priority queues

Internetworking protocols:

- Bridging:

- IEEE 802.1s Multiple Spanning Tree

- IEEE 802.1w Rapid Spanning Tree

- IEEE 802.1D Spanning Tree compatible

- IEEE 802.1Q – GVRP

Ring

- IP Multicast:

- IGMP Snooping

- Rate Control

- NTP

Network Management Methods

- Console port access via RS-232 cable (CLI, Command-Line Interface)
- Telnet remote access
- SNMP agent:

- MIB-2 (RFC1213)
- Bridge MIB (RFC1493)
- RMON MIB (RFC2819) – statistics, history, alarms, and events
- VLAN MIB (IEEE802.1Q/RFC2674)
- Private MIB
- Web browser
- TFTP software-upgrade capability

2.2.2 LEH900 Series Also Has…

- Complies with EN50121-4 environmental requirements for railway applications.
- Manageable via SNMP, Web-based, Telnet, and RS-232 console port.
- Support 802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 10/100/1000Mbps, full/half-duplex; Auto MDI/MDIX.
- Operating voltage and Max. current consumption: 0.92 A @ 12 VDC, 0.46 A @ 24 VDC.
  Power consumption: 11 W Max.
- -40 to +167° F (-40 to +75° C) operating temperature range. Tested for functional operation @ -40 to +185° F (-40 to +85° C).

2.2.3 LEH1000 Series Also Has…

- Supports IEEE 802.3af Power over Ethernet (PoE) Power Sourcing Equipment (PSE).
- Includes redundant power inputs: 47 to 57 VDC terminal block and 47 to 57 VDC jack.
- Power consumption: Device 15 W max. (without PoE); PoE power budget: 123.2 W max., PoE power output:
  Ports 1–8: IEEE 802.3af: Up to 15.4 W/port, 47–57 VDC.
- RS-232 console, Telnet, SNMP v1 & v2c & v3, RMON, Web browser, and TFTP management.
- Supports IEEE 802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 1000-Mbps full duplex; 10/100-Mbps full-/half-duplex; Auto MDI/MDIX.
- 100BASE-FX: Multimode SC or ST type, single-mode SC or ST type. 100BASE-BX: WDM single-mode SC type.
- 1000BASE-SX/LX: Multimode or single-mode SC type. 1000BASE-BX: WDM single-mode SC type.
- Store-and-forward mechanism. Full wire-speed forwarding rate.
- Field Wiring Terminal: Use Copper Conductors Only, 60/75° C, 12-24 AWG torque value 7 lb-in.
- Operating voltage and Max. current consumption: 0.31 A @ 48 VDC. Power consumption: Power consumption: 230 W Max. (Full load with PoE), 15 W Max. (Without PoE).
- -40 to +167° F (-40 to +75° C) operating temperature range. Tested for functional operation @ -40 to +185° F (-40 to +85° C). UL508 Industrial Control Equipment certified Maximum Surrounding Air Temperature @ 167° F (75° C).
- Hardened metal case..

NOTE: Make sure to readjust RTC Time of this switch to function accurately after this switch has been powered off for over 72 hours.

2.2.4 LEH1100 Series Also Has…

- RS-232 console, Telnet, SNMP v1 & v2c & v3, RMON, Web Browser, and TFTP management.
- Includes redundant power inputs: 47 to 57 VDC terminal block and 47 to 57 VDC jack.
- Port 1–Port 4 support IEEE 802.3at Power over Ethernet (PoE+) Power Sourcing Equipment (PSE).
- Power consumption: Device 15 W max. (without PoE+); PoE+ power budget: 181.6 W max.; PoE+ power output: Ports 1–4: IEEE 802.3at: Up to 30 W/port, 50–57 VDC
- Supports IEEE 802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation, 1000-Mbps full duplex, 10-/100-Mbps full/half duplex, Auto MDI/MDIX.
- Store-and-forward mechanism. Full wire-speed forwarding rate.
- Operating voltage and Max. current consumption: 0.31 A @ 48 VDC. Power consumption: 230 W Max. (Full load with PoE), 15W Max. (Without PoE).
- Field Wiring Terminal: Use Copper Conductors Only, 60/75, 12-24 AWG torque value 7 lb-in.
- -40 to 167° F (-40 to +75° C) operating temperature range. Tested for functional operation @ -40 to +185° F (-40 to +85° C). UL508 Industrial Control Equipment certified Maximum Surrounding Air Temperature @ 167° F (75° C). s
- Hardened metal case.

2.2.5 LEH1200 Series Also Has…

- UL1604 (ISA 12.1201) Class 1 Div. 2 certified, explosion-resistant
- Complies with EN50121-4 environmental requirements for railway applications.
- Manageable via SNMP, Web-based, Telnet, and RS-232 console port.
- Support 802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 10/100/1000Mbps, full/half-duplex; Auto MDI/MDIX.
- Operating voltage and Max. current consumption: 0.92 A @ 12 VDC, 0.46 A @ 24 VDC. Power consumption: 11 W Max.
- -40 to +167° F (-40 to +75° C) operating temperature range. Tested for functional operation @ -40 to +185° F (-40 to +85° C).

2.3 What's Included

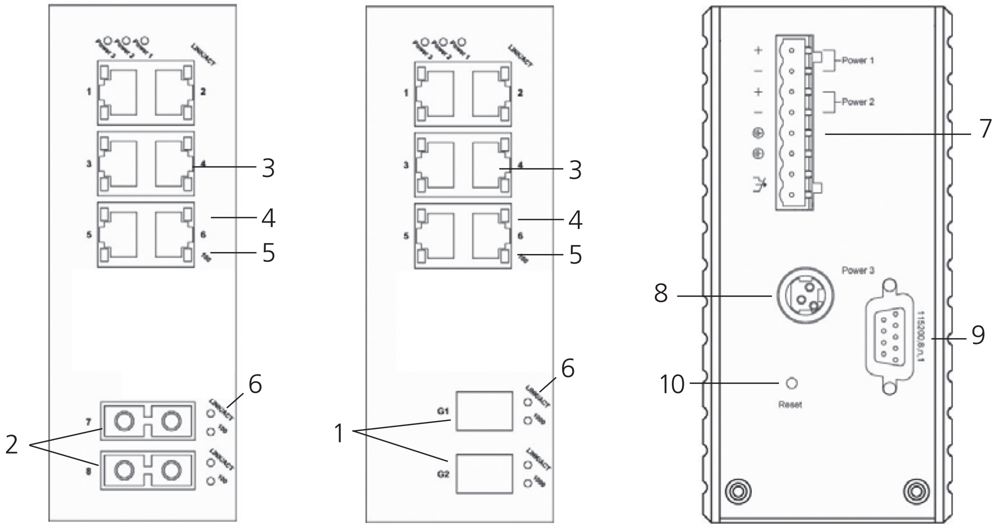
Your package includes the following items. If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

- Hardened Managed Ethernet Switch
- A quick start guide

NOTE: To download the user manual, go to www. blackbox.com, type the part number (from pages 10–11 of this manual) into the search bar and click on the Resources tab.

2.4 Hardware Description

2.4.1 LEH900 Series



Front panel of
LEH906A-2MMSC or
LEH906A-2MMST

Front panel of
LEH906A-2SFP or
LEH906A-2GSFP

Back panel (all models)

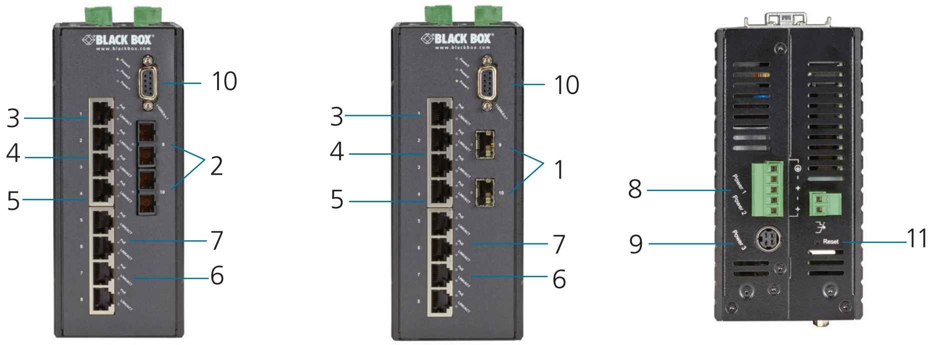
NOTE: LEH908A (not shown) has (8) RJ-45 ports and no ST, SC, or G1/G2 ports.

Figure 2-1. LEH900 Series Hardened Managed Ethernet Switch.

Table 2-2. LEH900 Series switches components.

Number in Figure 2-1	Product Name	Description
1	Ports G1 and G2	LEH906A-2GSFP: (2) GE SFP ports; LEH906A-2SFP: (2) SFP ports *NOTE: These connectors are not present on LEH906A-2MMSC and LEH906A-2MMST switches.*
2	(2) ST or SC fiber ports	LEH906A-2MMSC: (2) 10/100 MM SC ports; LEH906A-2MMST: (2) 10/100 MM ST ports *NOTE: These connectors are not present on LEH906A-2GSFP and LEH906A-2SFP switches.*
3	(6) RJ-45 ports	All LEH900 Series switches: 10/100 Mbps ports
4	(6) TX LEDs	See Table 2-5 for details.
5	(6) RX LEDs	See Table 2-5 for details.
6	Per port: (2) LINK/ACT LEDs	See Table 2-5 for details.
7	(1) Phoenix connector	Terminal block for Power 1, Power 2, and Ground
8	(1) DC power connector	Links to DC power source
9	(1) DB9 connector	Used for RS-232 serial control
10	(1) Reset button	Press to reset the switch to its defaults.

2.4.2 LEH1000 Series



Front panel of
LEH1008A-2MMSC or
LEH1008A-2MMST

Front panel of
LEH1008A-2SFP or
LEH1008A-2GSFP

Back panel (all models)

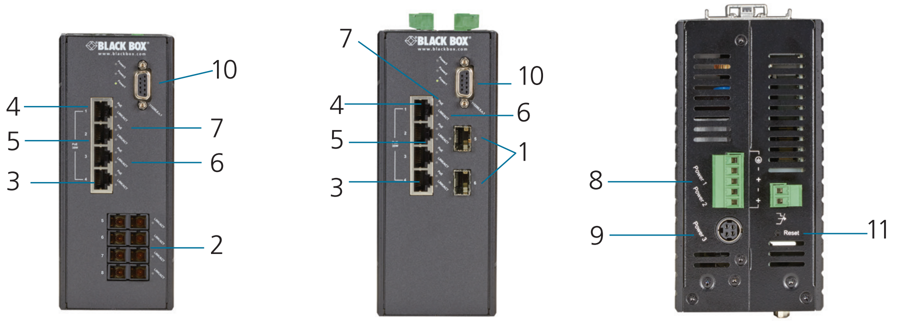
NOTE: LEH1008A (not shown) has (8) RJ-45 ports and no ST, SC, or G1/G2 ports.

Figure 2-2. LEH1000 Series Hardened Managed Ethernet Switch.

Table 2-2. LEH1000 Series switches components.

Number in Figure 2-2	Product Name	Description
1	Ports G1 and G2	LEH1008A-2GSFP: (2) GE SFP ports; LEH1008A-2SFP: (2) SFP ports *NOTE: These connectors are not present on LEH1000A-2MMSC and LEH1000A-2MMST switches.*
2	(2) ST or SC fiber ports	LEH1008A-2MMSC: (2) 10/100 MM SC ports; LEH1008A-2MMST: (2) 10/100 MM ST ports *NOTE: These connectors are not present on LEH1008A-2GSFP and LEH1008A-2SFP switches.*
3	(8) RJ-45 ports	All LEH1000 Series switches: 10/100 Mbps PoE ports
4	(8) TX LEDs	See Table 2-5 for details.
5	(8) RX LEDs	See Table 2-5 for details.
6	Per port: (2) LINK/ACT LEDs	See Table 2-5 for details.
7	Per port: (1) PoE LED	On when port is connected to a PoE PD (Powered Device)
8	(1) Phoenix connector	Terminal block for Power 1, Power 2, and Ground
9	(1) DC power connector	Links to DC power source
10	(1) DB9 connector	Used for RS-232 serial control
11	(1) Reset button	Press to reset the switch to its defaults.

2.4.3 LEH1100 Series



Front panel of
LEH1104A-4MMSC or
LEH1104A-4MMST

Front panel of
LEH1104A-2SFP or
LEH1104A-2GSFP

Back panel (all models)

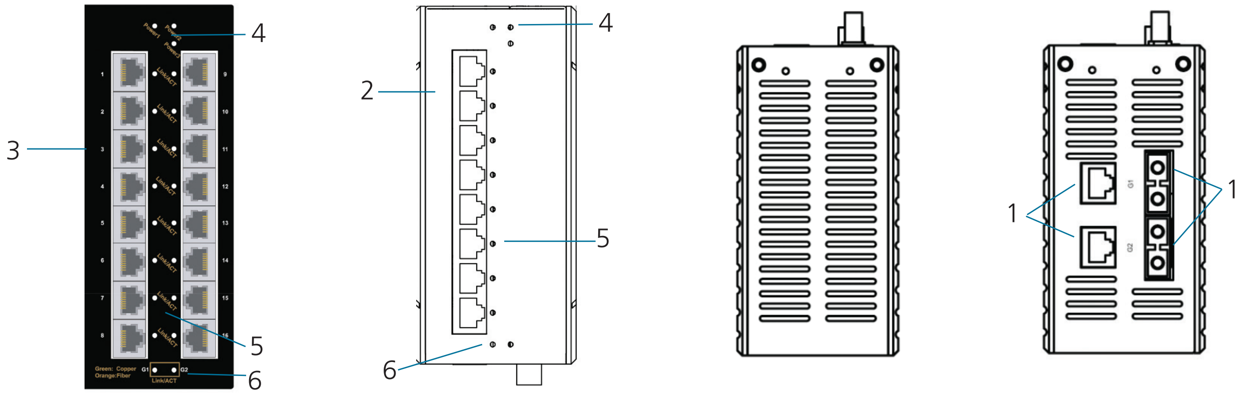
Figure 2-3. LEH1000 Series Hardened Managed Ethernet Switch.

Table 2-3. LEH1100 Series switches components.

Number in Figure 2-3	Product Name	Description
1	Ports G1 and G2	LEH1104A-2GSFP: (2) GE SFP ports; LEH1104A-2SFP: (2) SFP ports *NOTE: These connectors are not present on LEH1104A-2MMSC and LEH1104A-2MMST switches.*
2	(2) ST or SC fiber ports	LEH1104A-4MMSC: (2) 10/100 MM SC ports; LEH1104A-4MMST: (2) 10/100 MM ST ports *NOTE: These connectors are not present on LEH1104A-2GSFP and LEH1104A-2SFP switches.*
3	(4) RJ-45 ports	All LEH1000 Series switches: 10/100 Mbps PoE+ ports
4	(4) TX LEDs	See Table 2-5 for details.
5	(4) RX LEDs	See Table 2-5 for details.
6	Per port: (2) LINK/ACT LEDs	See Table 2-5 for details.
7	Per port: (1) PoE LED	On when port is connected to a PoE PD (Powered Device)
8	(1) Phoenix connector	Terminal block for Power 1, Power 2, and Ground
9	(1) DC power connector	Links to DC power source
10	(1) DB9 connector	Used for RS-232 serial control
11	(1) Reset button	Press to reset the switch to its defaults.

2.4.4 LEH1200 Series

Designed for rugged environments, these Hardened Managed Ethernet Switches provide reliable switching in industrial areas.

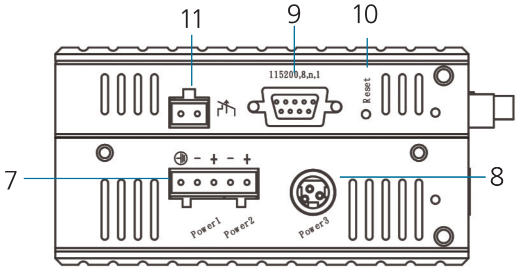


16-port RJ-45 or
16-port RJ-45 +
2 GMMSC/RJ-45
front view

8-port RJ-45 or
8-port RJ-45 +
2 GMMSC/RJ-45
front view

8-port RJ-45 or
16-port RJ-45
bottom view

8-port RJ-45 +
2 GMMSC/RJ-45 or
16-port RJ-45 +
2 GMMSC/RJ-45
bottom view



All models: top view.

Figure 2-4. LEH1200 Series Hardened Managed Ethernet Switch.

Table 2-4. LEH1200 Series switches components.

Number in Figure 2-4	Product Name	Description
1	Combo ports G1 and G2	LEH1208A-2GMMSC, LEH1216A-2GMMSC: (2) GE MMSC/RJ-45 combo ports *NOTE: These connectors are not present on LEH1208A and LEH1216A switches.*
2	(8) RJ-45 ports	LEH1208A and LEH1208A-2GMMSC switches: 10/100 Mbps ports
3	(16) RJ-45 ports	LEH1216A and LEH1216A-2GMMSC switches: 10/100 Mbps ports
4	(3) Power LEDs	See Table 2-6.
5	Per port: (1) LINK/ACT LED	See Table 2-6.
6	(2) LINK/ACT LEDs for combo ports	LEH1208A-2GMMSC and LEH1216A-2GMMSC only *NOTE: These LEDs are not present on LEH1208A and LEH1216A switches.*
7	(1) 5-pin terminal block	Terminal block for Power 1, Power 2, and Ground
8	(1) DC power connector	Links to DC power source
9	(1) DB9 connector	Used for RS-232 serial control
10	(1) Reset button	Press to reset the switch to factory defaults.
11	(1) 2-pin alarm contact	On relay output with current 1 A @ 24 VDC

2.4.5 Indicators on the LEH900, LEH1000, LEH1100, and LEH1200 Series Switches

Table 2-5. LEH900, LEH1000, and LEH1100 Series Switches Indicators.

LED	State	Indication
Power 1	Steady ON (Green)	Power ON
	Off	Power OFF
Power 2	Steady ON (Green)	Power ON
	Off	Power OFF
Power 3	Steady ON (Green)	Power ON
	Off	Power OFF
10/100BASE-TX, 100BASE-FX/BX		
LINK/ACT	Steady ON (Green)	A valid network connection is established
	Flashing	Transmitting or receiving data. *NOTE: ACT stands for activity.*
100	Steady ON (Green)	Connection at 100-Mbps speed.
10/100/1000BASE-SX/LX/BX		
LINK/ACT	Steady ON (Green)	A valid network connection is established
	Flashing	Transmitting or receiving data. *NOTE: ACT stands for activity.*
1000	Steady ON (Green)	Connection at 1000-Mbps speed.

Table 2-6. LEH1200 Series Switches Indicators.

LED	State	Indication
Power 1	Steady ON (Green)	Power ON
	Off	Power OFF
Power 2	Steady ON (Green)	Power ON
	Off	Power OFF
Power 3	Steady ON (Green)	Power ON
	Off	Power OFF
10/100BASE-TX, 100BASE-FX/BX (LED for 10/100-Mbps RJ-45 ports, #5 in Figure 1 on the previous page)		
LINK/ACT	Steady ON (Green)	A valid network connection is established.
	Flashing (Green)	Transmitting or receiving data. *NOTE: ACT stands for activity.*
10/100/1000BASE-SX/LX/BX (LED for GE MMSC/RJ-45 combo ports, #6 in Figure 1 on the previous page**)**		
LINK/ACT	Steady ON (Green)	A valid network connection is established on the copper port.
	Flashing (Green)	Transmitting or receiving data on the copper port. *NOTE: ACT stands for activity.*
	Steady ON (Orange)	A valid network connection is established on the fiber port.
	Flashing (Orange)	Transmitting or receiving data on the fiber port. *NOTE: ACT stands for activity.*

3. Installation

3.1 Selecting a Site for the Switch

As with any electric device, you should place the switch where it will not be subjected to extreme temperatures, humidity, or electromagnetic interference. Specifically, the site you select should meet the following requirements:

- The ambient temperature should be between -40 to +167° F (-40°C to +75° C).
- The relative humidity should be less than 95 percent, noncondensing.
- Surrounding electrical devices should not exceed the electromagnetic field (RFC) standards.
- Make sure that the switch receives adequate ventilation. Do not block the ventilation holes on each side of the switch.

3.2 Connecting to Power

Use redundant DC terminal block power inputs or 12-VDC jack.

3.2.1 12-VDC Jack

Step 1: Connect the supplied AC to DC power adapter to the receptacle on the top side of the switch.

Step 2: Connect the power cord to the AC to DC power adapter and attach the plug to a standard AC outlet with the appropriate AC voltage.

3.2.2 Redundant DC Terminal Block Power Inputs

There are two pairs of power inputs for use with redundant power sources. You only need to have one power input connected to run the switch.

Step 1: Connect the DC power cord to the pluggable terminal block on the switch, and then plug it into a standard DC outlet.

Step 2: Disconnect the power cord if you want to shut down the switch.

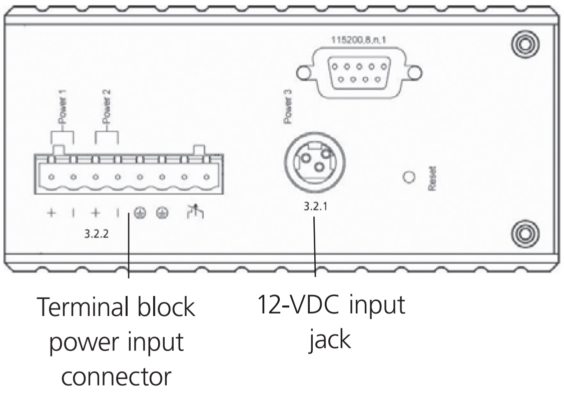


Figure 3-1. Top view.

3.2.3 Alarms for Power Failure

There are two pins on the terminal block used for power failure detection. It provides the normally closed output when the power source is active. Use this as a dry contact application to send a signal for power failure detection.

Table 3-1a. Power failure alarms for LEH900 and LEH1200 Series.

Power Input Assignment		
Power 3	12 VDC	DC jack
Power 2	+	12–48 VDC
	-	Power ground
Power 1	+	12–48 VDC
	-	Power ground
	Earth ground	
Relay output rating		1 A @ 24 VDC
Relay Alarm Assignment		
Fault	Warning signal disable for the following: • The relay contact closes if Power 1 and Power 2 both fail, but Power 3 is ON. • The relay contact closes if Power 3 fails, but Power 1 and Power 2 are ON.	

Table 3-1b. Power failure alarms for LEH1000 and LEH1100 Series.

Power Input Assignment		
Power 3	47 to 57 VDC	DC jack
Power 2	+	47–57 VDC
	-	Power ground
Power 1	+	47–57 VDC
	-	Power ground
	Earth ground	
Relay output rating		1 A @ 250 VAC
Relay Alarm Assignment		
Fault	Warning signal disable for the following: • The relay contact closes if Power 1 and Power 2 both fail, but Power 3 is ON. • The relay contact closes if Power 3 fails, but Power 1 and Power 2 are ON.	

NOTE: The relay output is normally in the open position when there is no power to the switch. Please do not connect any power source to this terminal to prevent shorting your power supply.

3.3 Connecting to Your Network

3.3.1 Cable Type and Length

Follow the cable specifications below when connecting the switch to your network. Use appropriate cables that meet your speed and cabling requirements.

Table 3-2. Cable specifications.

Speed	Connector	Port Speed (Half/Full Duplex)	Cable	Maximum Distance
10BASE-T	RJ-45	10/20 Mbps	2-pair UTP/STP CAT3, 4, 5	328 feet (100 m)
100BASE-TX	RJ-45	100/200 Mbps	2-pair UTP/STP CAT5	328 feet (100 m)
1000BASE-T	RJ-45	2000 Mbps	4-pair UTP/STP CAT5	328 feet (100 m)
100BASE-FX	ST, SC	200 Mbps	62.5-µm multimode fiber	2 km
100BASE-FX	ST, SC	200 Mbps	10-µm single-mode fiber	20, 40 km
100BASE-BX	SC	200 Mbps	62.5-µm multimode fiber	2 km
100BASE-BX	SC	200 Mbps	10-µm single-mode fiber	20, 40 km
1000BASE-SX	SC	2000 Mbps	62.5-µm multimode fiber	220 m, 2 km
1000BASE-SX	SC	2000 Mbps	50-µm multimode fiber	550 m
1000BASE-LX	SC	2000 Mbps	10–µm single-mode fiber	10, 20, 50 km
1000BASE-LX	SC	2000 Mbps	10–µm single-mode fiber	20, 40 km
SFP				
1000BASE-SX	Duplex LC	2000 Mbps	62.5-µm multimode fiber	550 m, 2 km
1000BASE-LX	Duplex LC	2000 Mbps	9–µm single-mode fiber	10, 40, 60 km
1000BASE-BX	Duplex LC	2000 Mbps	9–µm single-mode fiber	70 km

3.3.2 Cabling

Step 1: First, ensure the power of the switch and end devices are turned off.

NOTE: Always ensure that the power is off before any installation.

Step 2: Prepare cable with corresponding connectors for each type of port in use.

Step 3: Consult the Cable specifications table (above) for cabling requirements based on connectors and speed.

Step 4: Connect one end of the cable to the switch and the other end to a desired device.

Step 5: Once the connections between two end devices are made successfully, turn on the power and the switch is operational.

4. Switch Management

This chapter explains the methods that you can use to configure management access to the switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

4.1 Management Access Overview

The switch gives you the flexibility to access and manage the switch using any or all of the following methods.

The Web browser interface and administration console (CLI) support are embedded in the switch software and are available for immediate use.

4.2 Administration Console (CLI)

The administration console is an internal, character-oriented, Command-Line Interface (CLI) for performing system administration such as displaying statistics or changing option settings.

Using this method, you can view the administration console from a terminal, personal computer, Apple® Macintosh´®, or workstation connected to the switch's console port.

There are two ways to use this management method: direct access or modem access. The following sections describe these methods.

4.2.1 Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

When using the management method, configure the terminal-emulation program to use the following parameters (you can change these settings after login):

Default parameters:

- 115,200 bps
- 8 data bits
- No parity
- 1 stop bit

This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX® can use an emulator such as TIP.

4.2.2 Modem Access

You can access the switch's administration console from a PC or Macintosh using an external modem attached to the console port. The switch management program provides the Console Port screen, accessible from the Basic Management screen that lets you configure parameters for modem access.

When you have configured the external modem from the administration console, the switch transmits characters that you have entered as output on the modem port. The switch echoes characters that it receives as input on the modem port to the current administration console session. The console appears to be directly connected to the external modem.

4.3 Web Management

The switch provides a browser interface that lets you configure and manage the switch remotely.

After you set up your IP address for the switch, you can access the switch's Web interface applications directly in your Web browser by entering the IP address of the switch. You can then use your Web browser to list and manage switch configuration parameters from one central location, just as if you were directly connected to the switch's console port.

4.4 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the switch. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Network management station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default get and set community strings for the switch are public.

4.5 Protocols

The switch supports the following protocols:

Virtual terminal protocols, such as Telnet

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the switch before you can establish access to it with a virtual terminal protocol.

NOTE: Terminal emulation is different from a virtual terminal protocol in that you must connect a terminal directly to the console port.

Simple Network Management Protocol (SNMP)

SNMP is the standard management protocol for multivendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

4.6 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (e.g., console port) are immediately displayed by the other management methods (e.g., SNMP agent of Web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the switch is compatible with, and will interoperate with, other solutions that adhere to the same open standard.

5. SNMP and RMON Management

This chapter describes the switch's Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) capabilities.

5.1 Overview

RMON is an abbreviation for the Remote Monitoring MIB (Management Information Base). RMON is a system defined by the Internet Engineering Task Force (IETF) document RFC 2819, which defines how networks can be monitored remotely.

RMONs typically consist of two components: an RMON probe and a management workstation:

- The RMON probe is an intelligent device or software agent that continually collects statistics about a LAN segment or VLAN. The RMON probe transfers the collected data to a management workstation on request or when a pre-defined threshold is reached.
- The management workstation collects the statistics that the RMON probe gathers. The workstation can reside on the same network as the probe, or it can have an in-band or out-of-band connection to the probe.

The switch provides RMON capabilities that allow network administrators to set parameters and view statistical counters defined in MIB-II, Bridge MIB, and RMON MIB. RMON activities are performed at a Network Management Station running an SNMP network management application with graphical user interface.

5.2 SNMP Agent and MIB-2 (RFC 1213)

The SNMP Agent running on the switch manager CPU is responsible for:

- Retrieving MIB counters from various layers of software modules according to the SNMP GET/GET NEXT frame messages.
- Setting MIB variables according to the SNMP SET frame message.
- Generating an SNMP TRAP frame message to the Network Management Station if the threshold of a certain MIB counter is reached or if other trap conditions (such as the following) are met:

WARM START

COLD START

LINK UP

LINK DOWN

AUTHENTICATION FAILURE

RISING ALARM

FALLING ALARM

TOPOLOGY ALARM

MIB-II defines a set of manageable objects in various layers of the TCP/IP protocol suites. MIB-II covers all manageable objects from layer 1 to layer 4, and, as a result, is the major SNMP MIB supported by all vendors in the networking industry. The switch supports a complete implementation of SNMP Agent and MIB-II.

5.3 RMON MIB (RFC 2819) and Bridge MIB (RFC 1493)

The switch provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that complies with the RMON MIB definition.

5.4 RMON Groups Supported

The switch supports the following RMON MIB groups defined in RFC 2819:

- RMON Statistics Group – maintains usage and error statistics for the switch port being monitored.
- RMON History Group – gathers and stores periodic statistical samples from the previous Statistics Group.

- RMON Alarm Group – allows a network administrator to define alarm thresholds for any MIB variable. An alarm can be associated with Low Threshold, High Threshold, or both. A trigger can trigger an alarm when the value of a specific MIB variable exceeds or falls below a threshold.
- RMON Event Group – allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered. The action taken in the Network Management Station depends on the specific network management application.

5.5 Bridge Groups Supported

The switch supports the following four groups of Bridge MIB (RFC 1493):

- The dot1dBase Group – a mandatory group that contains the objects applicable to all types of bridges.
- The dot1dStp Group – contains objects that denote the bridge's state with respect to the Spanning Tree Protocol. If a node does not implement the Spanning Tree Protocol, this group will not be implemented. This group is applicable to any transparent only, source route, or SRT bridge that implements the Spanning Tree Protocol.
- The dot1dTp Group – contains objects that describe the entity's transparent bridging status. This group is applicable to transparent operation only and SRT bridges.
- The dot1dStatic Group – contains objects that describe the entity's destination-address filtering status. This group is applicable to any type of bridge that performs destination-address filtering.

6. Web-Based Browser Management

The switch provides a Web-based browser interface for configuring and managing the switch. This interface allows you to access the switch using a preferred Web browser.

This chapter describes how to configure the switch using its Web-based browser interface.

6.1 Logging on to the Switch

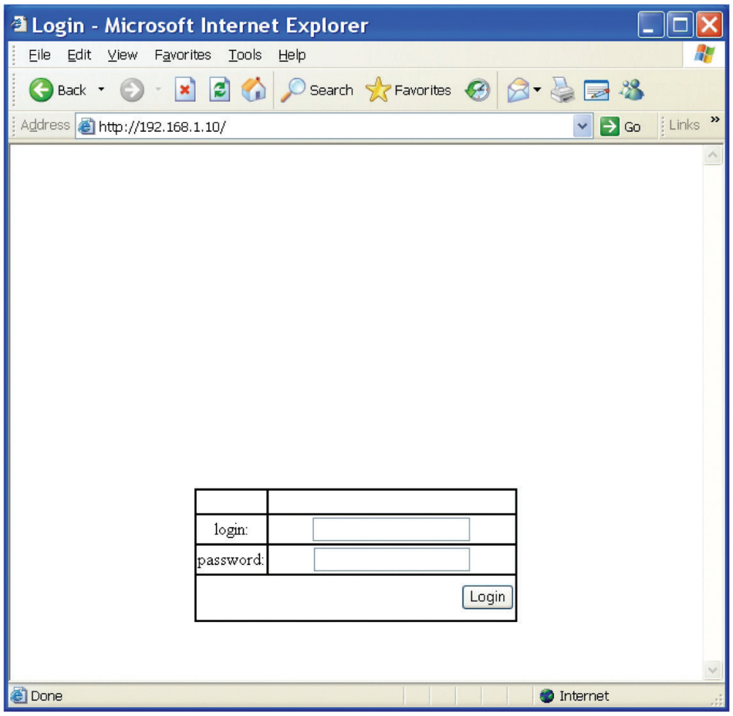

Login - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://192.168.1.10/
Go
Links
login:
password:
Login
Done
Internet

Figure 6-1. Logging on to the switch.

Switch IP address

In your Web browser, specify the IP address of the switch. Default IP address is 192.168.1.10.

Login

Enter the factory default login ID: root.

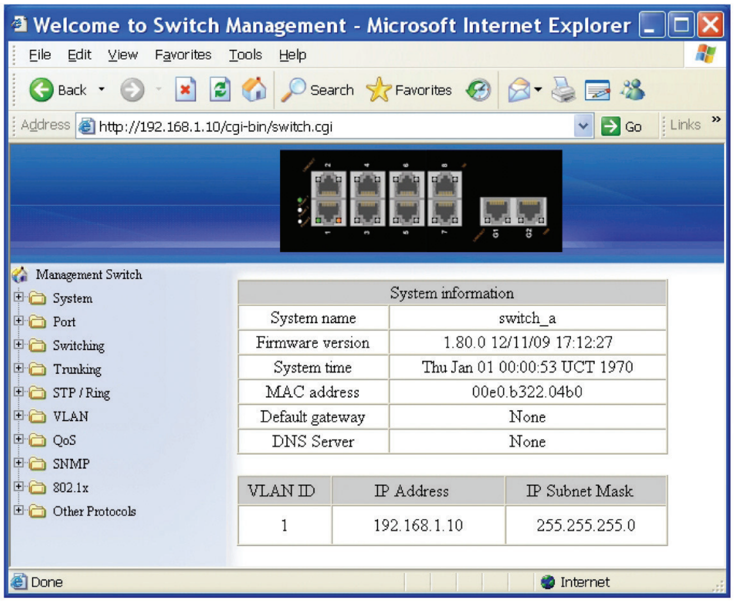
Password

Enter the factory default password (no password). Or enter a user-defined password if you followed the instructions later and changed the factory default password.

Then click on the "Login" button to log on to the switch.

6.2 Understanding the Browser Interface

The Web browser interface provides groups of point-and-click buttons at the left field of the screen for configuring and managing the switch.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

System information	
System name	switch_a
Firmware version	1.80.0 12/11/09 17:12:27
System time	Thu Jan 01 00:00:53 UCT 1970
MAC address	00e0.b322.04b0
Default gateway	None
DNS Server	None

VLAN ID	IP Address	IP Subnet Mask
1	192.168.1.10	255.255.255.0

Figure 6-2. Browser interface.

System

System Information, System Name/Password, IP Address, Save Configuration, Firmware Upgrade, Reboot, Logout, User Account, User Privilege

Diagnostics

Utilization, System Log, Remote Logging, ARP Table, Route Table, Alarm Setting

Port

Configuration, Port Status, Rate Control, RMON Statistics, Per Port VLAN Activities

Switching

Bridging, Loopback Detect, Static MAC Entry, Port Mirroring, Link State Tracking, PoE, PoE Scheduling

Trunking

Port Trunking, LACP Trunking

STP/RING

Global Configuration, RSTP Port Setting, MSTP Properties, MSTP Instance Setting, MSTP Port Setting, Ring Setting, Chain Setting, Chain Pass-Through Setting, Advanced Setting

VLAN

VLAN Mode Setting, 802.1Q VLAN Setting, 802.1Q Port Setting, Port Based VLAN

QOS

Global Configuration, 802.1p Priority, DSCP

SNMP

SNMP General Setting, SNMP v1/v2c, SNMP v3

802.1X

Radius Configuration, Port Authentication

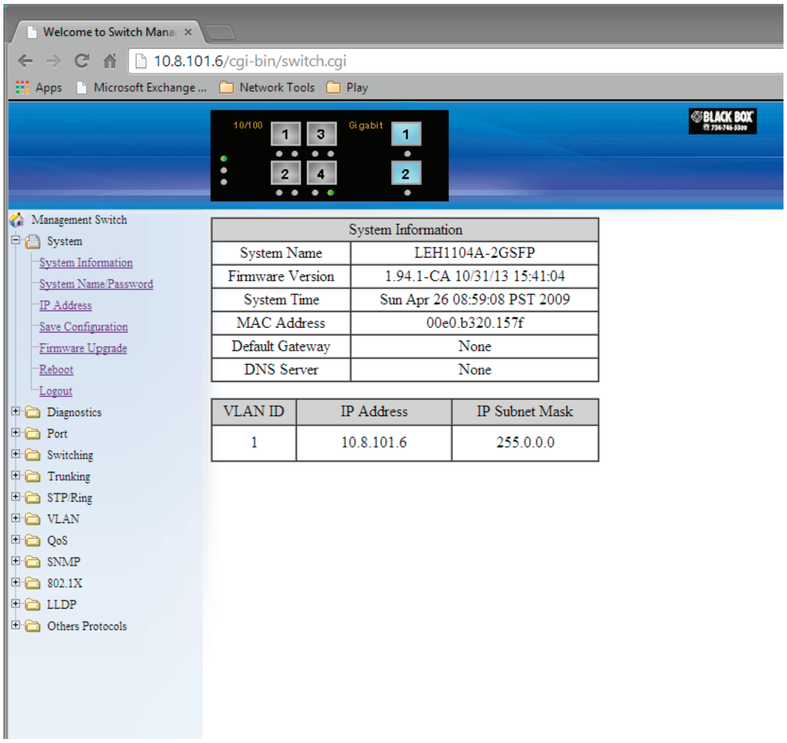
LLDP

LLDP General Settings, LLDP Porsts Settings, LLDP Neighbors, LLDP Statistics

Other Protocols

GVRP, IGMP Snooping, NTP, GMRP, DHCP Server

6.3 System


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

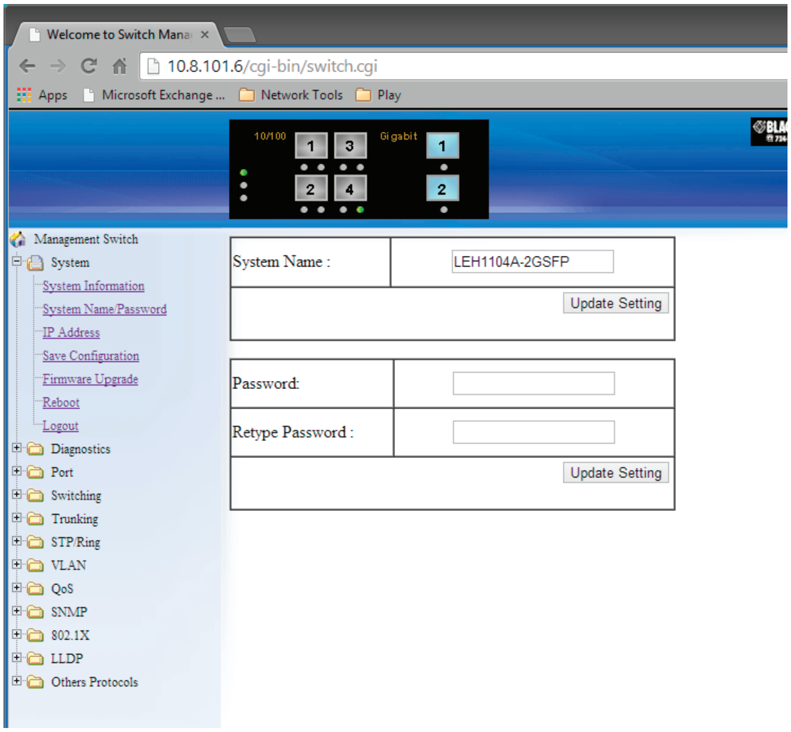
System Information	
System Name	LEH1104A-2GSFP
Firmware Version	1.94.1-CA 10/31/13 15:41:04
System Time	Sun Apr 26 08:59:08 PST 2009
MAC Address	00e0.b320.157f
Default Gateway	None
DNS Server	None

VLAN ID	IP Address	IP Subnet Mask
1	10.8.101.6	255.0.0.0

Figure 6-3. System screen.

System Information

The System Name, Firmware Version, System Time, MAC Address, Default Gateway, DNS Server, VLAN ID, IP Address, IP Subnet Mask, and Current User Information of Switch.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Update Setting
Update Setting

System Name : LEH1104A-2GSFP

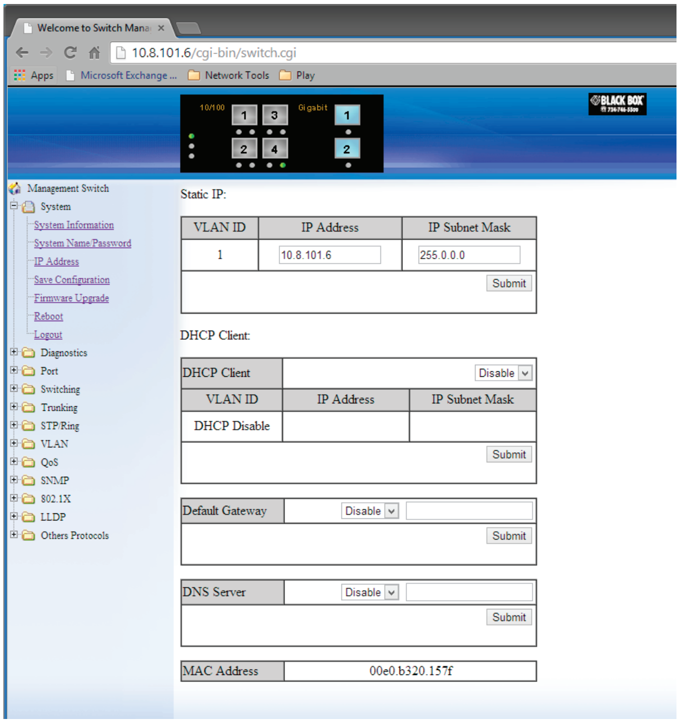
Password:

Retype Password :

Figure 6-4. System name/password screen.

System Name/Password

1. System Name: Click in the "System Name" text box. Type a system name if it is blank, or replace the current system name with a new one.
2. Update Setting: Click the "Update Setting" button to update your settings.
3. Password: Click in the "Password" text box. Type a password.
4. Retype Password: Click in the "Retype Password" text box. Type the same password in the "Password" text box again to verify it.
5. Update Setting: Click the "Update Setting" button to update your settings.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
724-746-5500
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Submit

Static IP:

VLAN ID	IP Address	IP Subnet Mask
1	10.8.101.6	255.0.0.0

DHCP Client:

DHCP Client		Disable
VLAN ID	IP Address	IP Subnet Mask
DHCP Disable		

Default Gateway	Disable	

DNS Server	Disable	

MAC Address	00e0.b320.157f

Figure 6-5. IP address screen.

IP Address

1. IP Address: Click in the “IP Address” text box and type a new address to change the IP Address.

2. IP Subnet Mask: Click in the “IP Subnet Mask” text box and type a new address to change the IP Subnet Mask.

3. Submit: Click the “Submit” button after you finish these selections.

4. You need to enter the new IP address on the browser and reconnect to the switch after the IP or subnet mask is changed.

5. DHCP Client: Click the “DHCP Client” drop-down menu to choose “Disable” or “VLAN1” (or other VLAN group) from the “DHCP Client” drop-down list to disable or enable DHCP Client Setting for the switch. The managed VLAN is VLAN 1 by default. The managed IP Address will be assigned by DHCP Server when VLAN 1 is chosen as DHCP Client. DHCP Server can assign the Switch another managed IP Address by choosing another VLAN besides VLAN 1 as DHCP Client when the switch has multiple VLANs.

6. Submit: Click the “Submit” button after you finish configuring DHCP Client.

7. Default Gateway: Choose “Disable” or “Enable” from the “Default Gateway” drop-down list to disable or enable Default Gateway Setting for the switch.

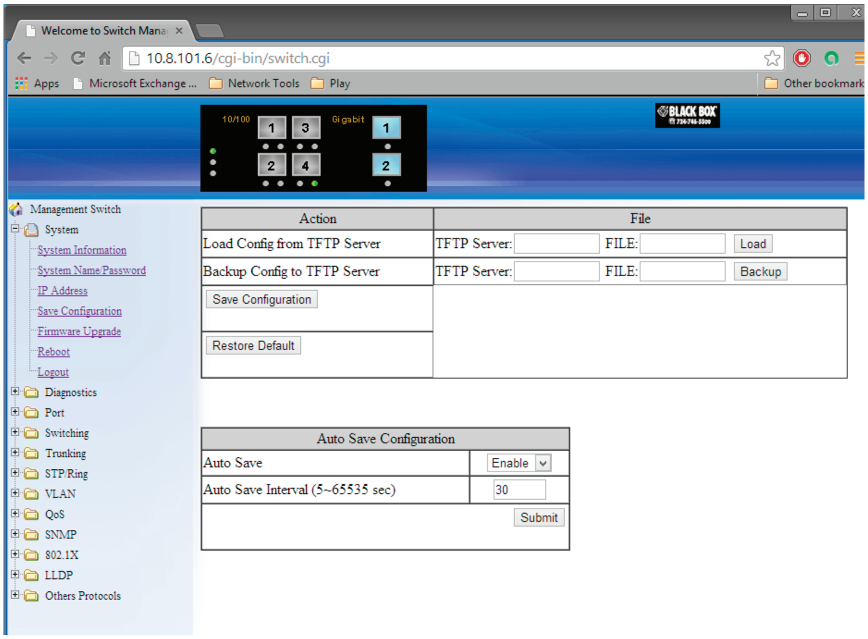
   Click the text box and type a new address to change the Default Gateway. (You need to choose “Enable” from the “Default Gateway” drop-down menu.)

8. Submit: Click “Submit” button after you finish configuring Default Gateway.

9. DNS Server: Click the “DNS Server” drop-down menu to choose “Disable” or “Enable” from the “DNS Server” drop-down list to disable or enable DNS Server Setting for the switch.

   Click the text box and type a new address to change the DNS Server. (Need to choose “Enable” from the “DNS Server” drop-down menu.)

10. Submit: Click the “Submit” button after you finish configuring DNS Server.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
Other bookmark
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

Action	File
Load Config from TFTP Server	TFTP Server: ☐ FILE: ☐ Load
Backup Config to TFTP Server	TFTP Server: ☐ FILE: ☐ Backup
Save Configuration	
Restore Default	

Auto Save Configuration	
Auto Save	Enable
Auto Save Interval (5~65535 sec)	30
	Submit

Figure 6-6. Save configuration screen.

Save Configuration

1. Load Config from TFTP Server:

Click in the "TFTP Server" text box and type the TFTP server IP address from where the file will be obtained.

Click in the "FILE" text box and type the name of the file that will be obtained.

Click the "Load" button to load the file from the TFTP server.

2. Backup Config to TFTP Server:

Click in the "TFTP Server" text box and type the TFTP server IP address to where the file will be backed up.

Click in the "FILE" text box and type the name of the file that will be backupped.

Click the "Backup" button to backup the file to the TFTP server.

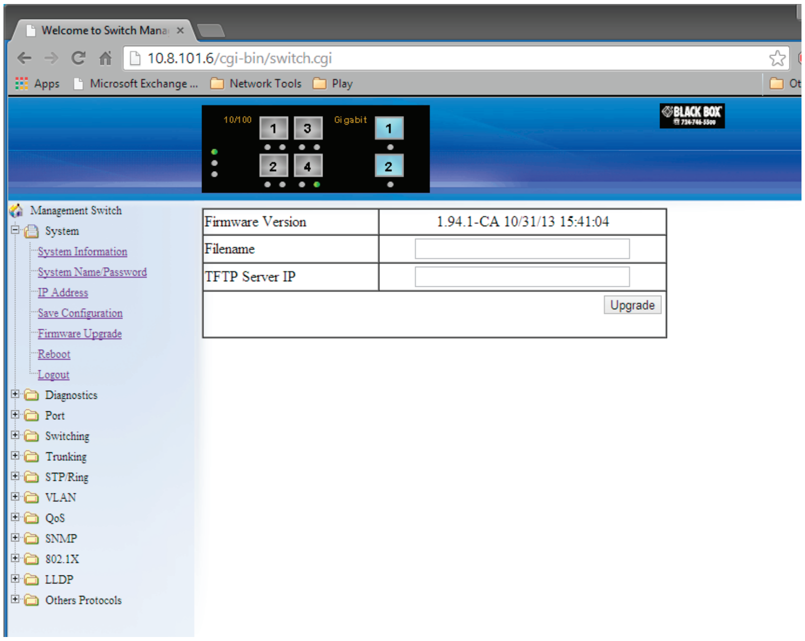
3. Save Configuration: Click "Save Configuration" button to save your configuration settings.

4. Restore Default: Click "Restore Default" button to restore the default settings of the switch.

5. Auto Save: Click the "Auto Save" drop-down menu to choose "Disable" or "Enable" from the "Auto Save" drop-down list to disable or enable Auto Save for the switch.

6. Auto Save Interval (5–65536 sec): Click in the "Auto Save Interval" text box and type a decimal number between 5 and 65536.

7. Submit: Click the "Submit" button when you finish the Auto Save configuration.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Upgrade

Firmware Version	1.94.1-CA 10/31/13 15:41:04
Filename	
TFTP Server IP	

Figure 6-7.

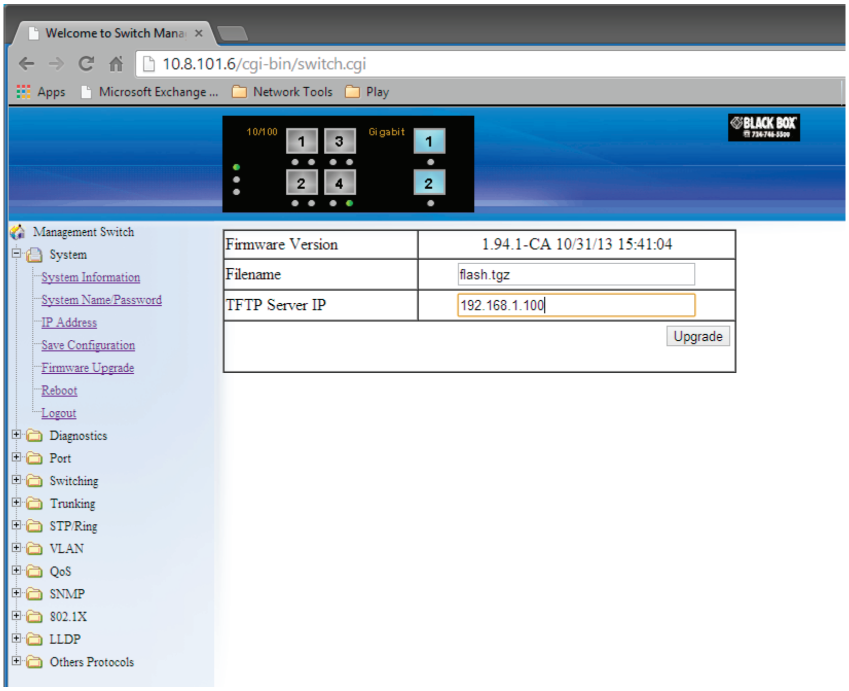
Firmware Upgrade

1. Filename: Click in the "Filename" text box and type the name of the file that you intend to upgrade to the switch.

2. TFTP Server IP: Click in the "TFTP Server IP" text box and type the TFTP server IP address from where the file will be obtained.

3. Upgrade: Click the "Upgrade" button to upgrade firmware to the switch.

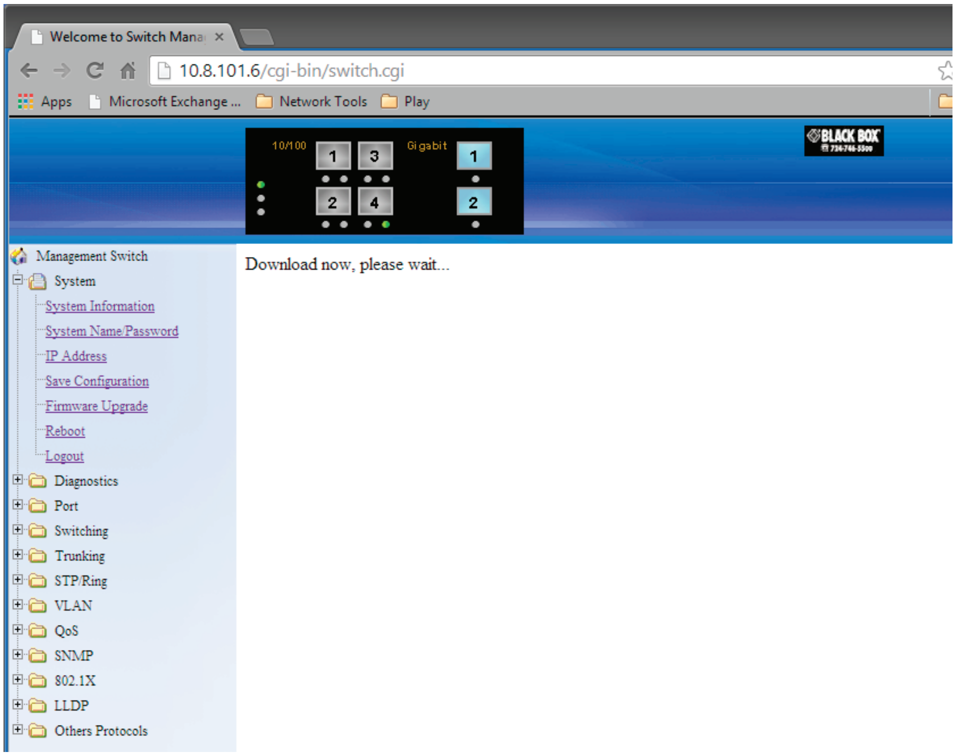
Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time. Reboot the switch after completing the upgrade process.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Upgrade

Firmware Version	1.94.1-CA 10/31/13 15:41:04
Filename	flash.tgz
TFTP Server IP	192.168.1.100

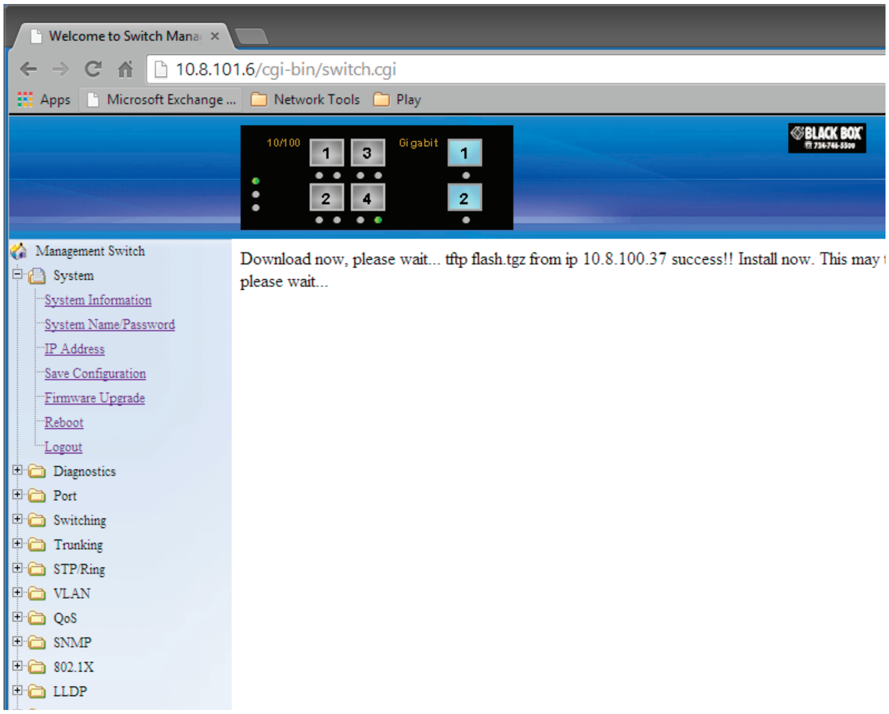
FIgure 6-8.

Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

Download now, please wait...

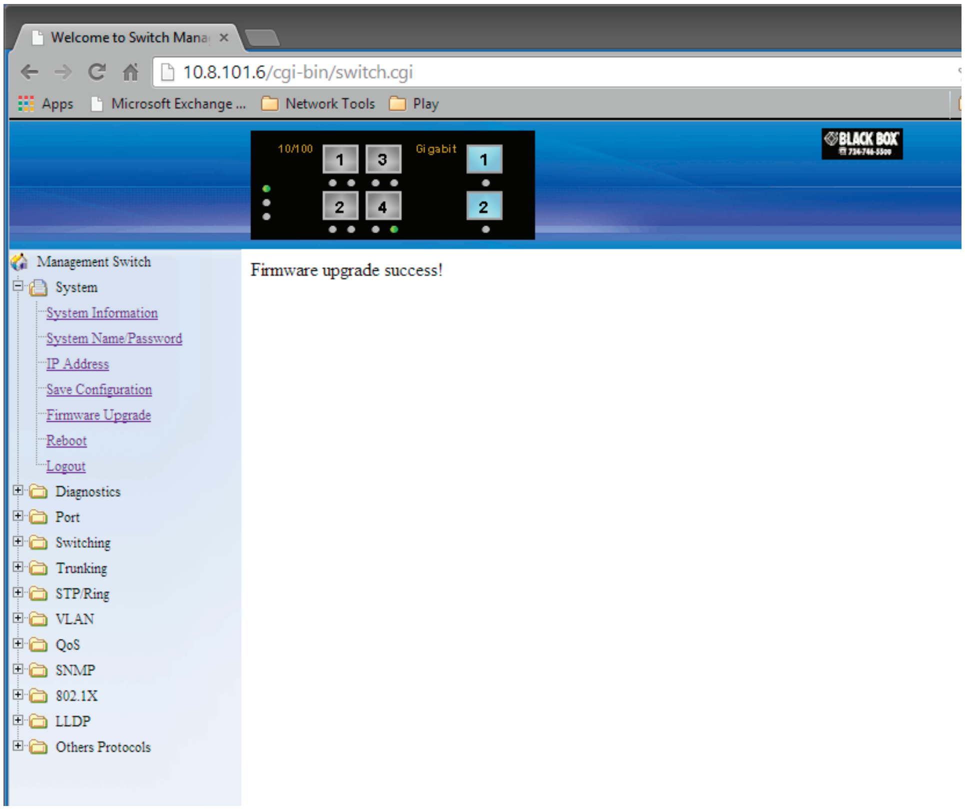
Figure 6-9.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP

Download now, please wait... tftp flash.tgz from ip 10.8.100.37 success!! Install now. This may
please wait...

Figure 6-10.

Firmware has been upgraded successfully to the switch. Reboot the switch after completing the upgrade process.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

Firmware upgrade success!

Figure 6-11.

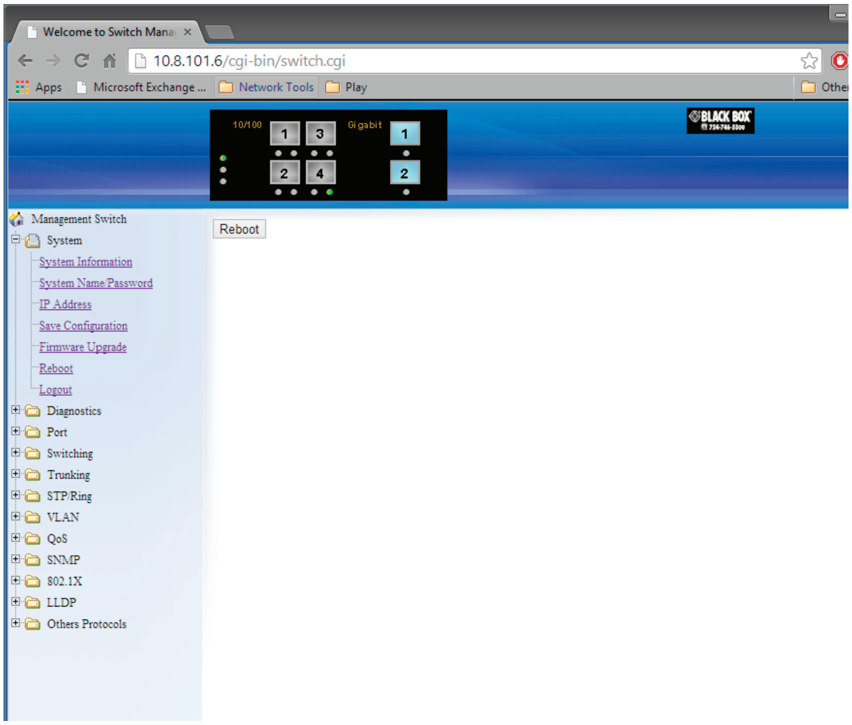
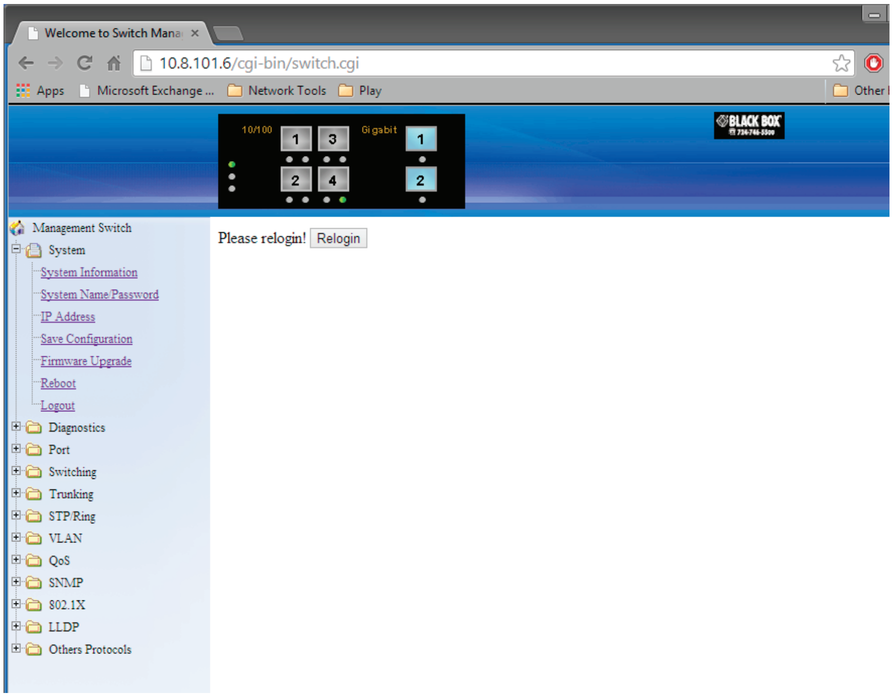

Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
Othe
10/100
Gigabit
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Reboot

Figure 6-12.

Reboot: Click the "Reboot" button to restart the switch.

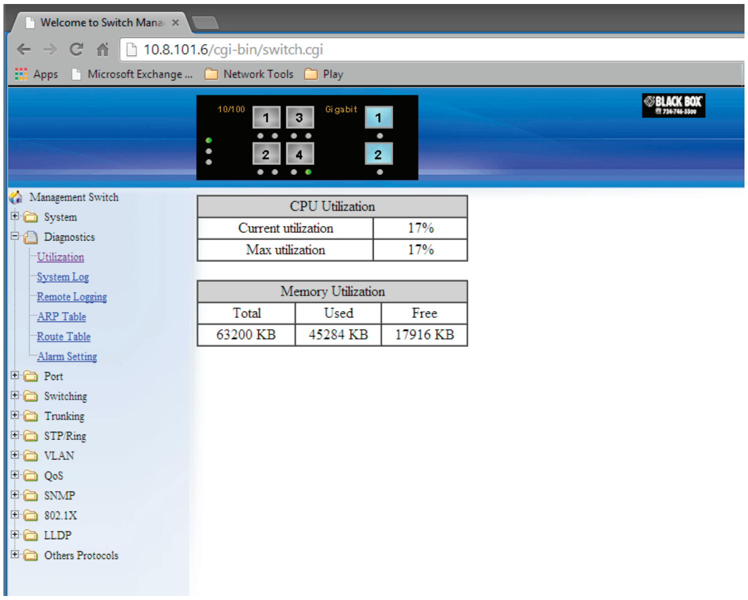

Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
Other
10/100
Gigabit
BLACK BOX
Management Switch
System
System Information
System Name/Password
IP Address
Save Configuration
Firmware Upgrade
Reboot
Logout
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Relogin

Please relogin!

Figure 6-13. Logout button.

Logout: Click on the "Relogin" button to log back into the switch.

6.4 Diagnostics


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
Diagnostics
Utilization
System Log
Remote Logging
ARP Table
Route Table
Alarm Setting
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

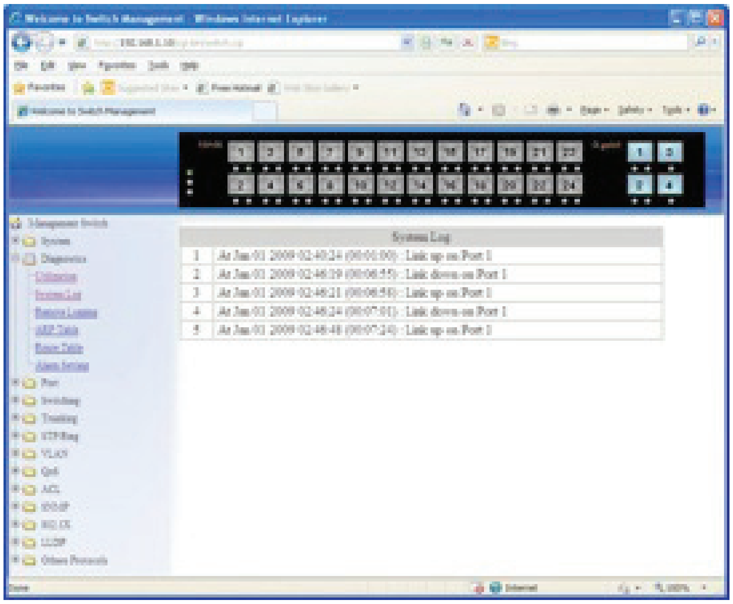
CPU Utilization	
Current utilization	17%
Max utilization	17%

Memory Utilization		
Total	Used	Free
63200 KB	45284 KB	17916 KB

Figure 6-14.

Utilization

Click Utilization to view CPU Utilization and Memory Utilization.



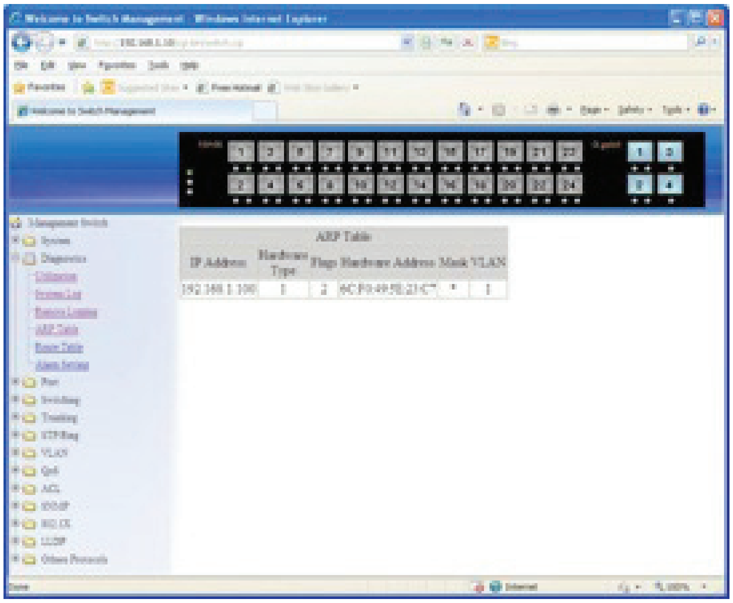
System Log

```
1  At Jan 01 2009 02:40:24 (00:01:00) : Link up on Port 1
2  At Jan 01 2009 02:46:19 (00:06:55) : Link down on Port 1
3  At Jan 01 2009 02:46:21 (00:06:58) : Link up on Port 1
4  At Jan 01 2009 02:46:24 (00:07:01) : Link down on Port 1
5  At Jan 01 2009 02:46:48 (00:07:24) : Link up on Port 1
```

Figure 6-15.

System Log

Click System Log to view system log.



ARP Table

IP Address	Hardware Type	Flags	Hardware Address	Mask	VLAN
192.168.1.100	1	2	8C:F0:49:5E:21:C7	*	1

Figure 6-16.

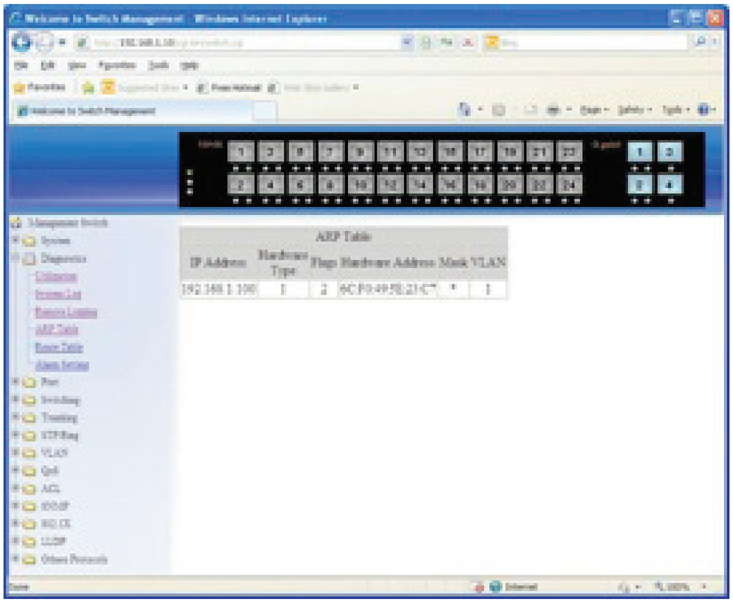
Remote Logging

1. Status: Click and choose “Enable” or “Disable” to enable or disable the logging of messages that are sent to syslog servers.

2. Update Setting: Click “Update Setting” button to update your settings.

3. Syslog Server IP: Click in “Syslog Server IP” text box and type a syslog server IP address.

4. Add Syslog Server: Click "Add Syslog Server" button to add a syslog server.
5. Syslog Server IP List: Click "Syslog Server IP List" drop-down menu and choose a syslog server IP address from the "Syslog Server IP List" drop-down list to be deleted.
6. Delete Syslog Server: Click "Delete Syslog Server" button to delete a syslog server.


Management Switch
System
Diagnostics
Utilization
System Log
Remote Logging
ARP Table
Route Table
Alarm Setting
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
IGMP
802.1X
LLDP
Others Protocols

ARP Table

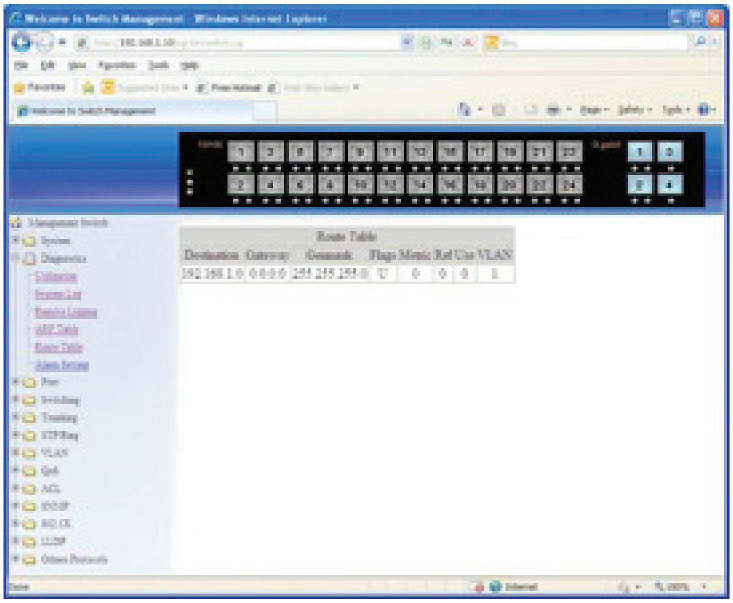
IP Address	Hardware Type	Flags	Hardware Address	Mask	VLAN
192.168.1.100	1	2	6C:F0:49:5E:21:C7	*	1

Figure 6-17.

ARP Table

Click ARP Table to view ARP Table.

The ARP Table is learned by Switch CPU, not learned by Switch MAC. The MAC Address of PC that have accessed Switch user interface will be recorded in the ARP Table.


Management Switch
System
Diagnostics
Utilization
System Log
Remote Logging
ARP Table
Route Table
Alarm Setting
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
IGMP
802.1X
LLDP
Others Protocols

Route Table

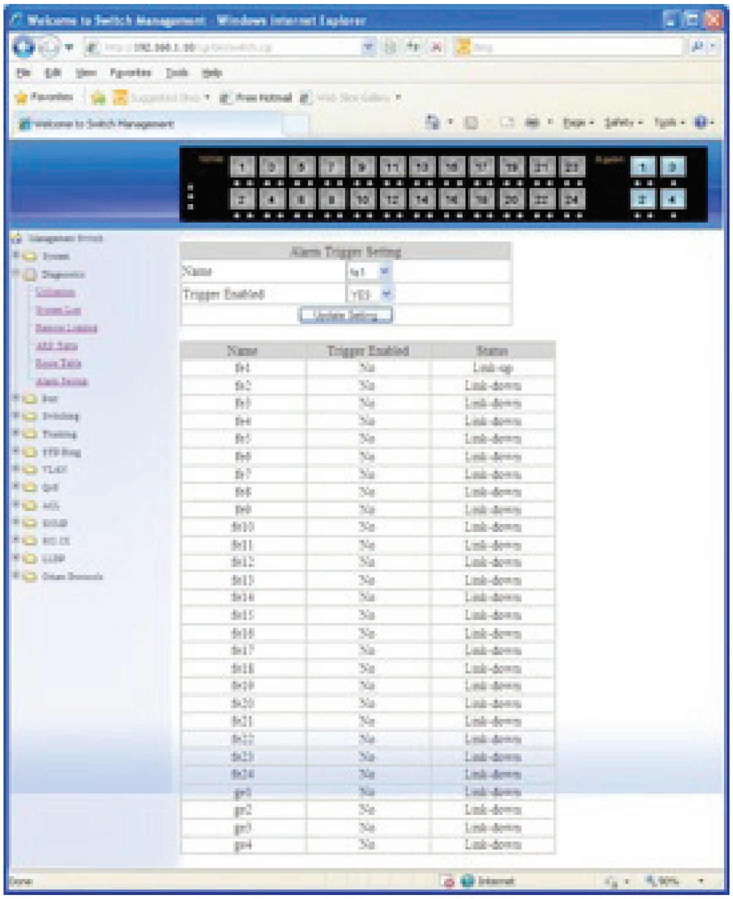
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	VLAN
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	1

Figure 6-18.

Route Table

Click Route Table to view Route Table.

Route Table lists the routes to network destinations. And metrics (distances) are associated with those routes. The Route Table contains information about the topology of the network around it.



Alarm Trigger Setting

Name: fe1

Trigger Enabled: YES

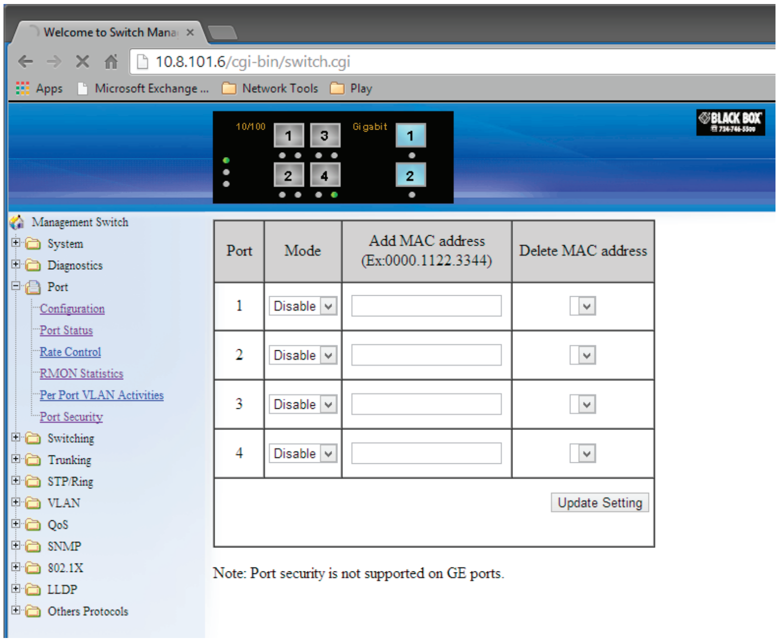
Name	Trigger Enabled	Status
fe1	No	Link-up
fe2	No	Link-down
fe3	No	Link-down
fe4	No	Link-down
fe5	No	Link-down
fe6	No	Link-down
fe7	No	Link-down
fe8	No	Link-down
fe9	No	Link-down
fe10	No	Link-down
fe11	No	Link-down
fe12	No	Link-down
fe13	No	Link-down
fe14	No	Link-down
fe15	No	Link-down
fe16	No	Link-down
fe17	No	Link-down
fe18	No	Link-down
fe19	No	Link-down
fe20	No	Link-down
fe21	No	Link-down
fe22	No	Link-down
fe23	No	Link-down
fe24	No	Link-down
ge1	No	Link-down
ge2	No	Link-down
ge3	No	Link-down
ge4	No	Link-down

Figure 6-19.

Alarm Setting

1. Name: Click on the "Name" drop-down menu to choose "fe1–fe8," "ge1–ge2," or "Power 1–Power 3" from the "Name" drop-down list.
2. Trigger Enabled: Choose "Yes" or "No" from the "Trigger Enabled" drop-down list to enable or disable Trigger.
3. Update setting: Click on the "Update Setting" button to update settings to the switch.

6.5 Port


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Update Setting

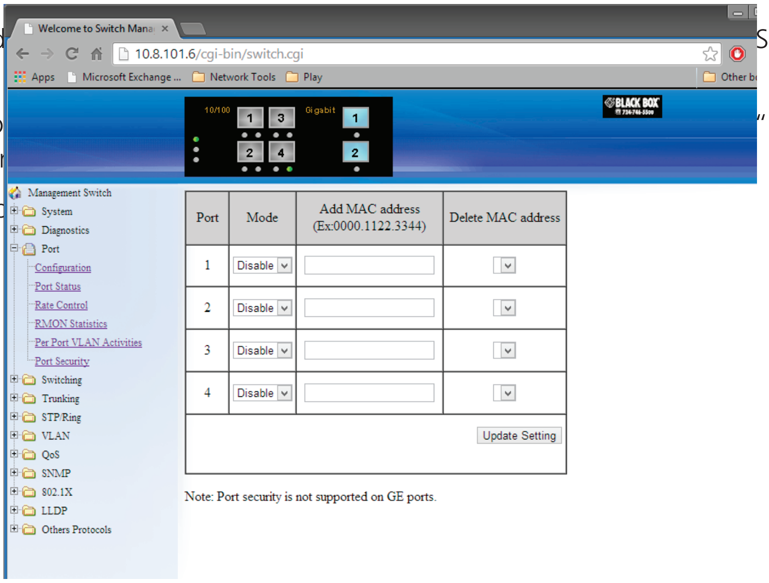
Port	Mode	Add MAC address (Ex:0000.1122.3344)	Delete MAC address
1	Disable		
2	Disable		
3	Disable		
4	Disable		

Note: Port security is not supported on GE ports.

Figure 6-20.

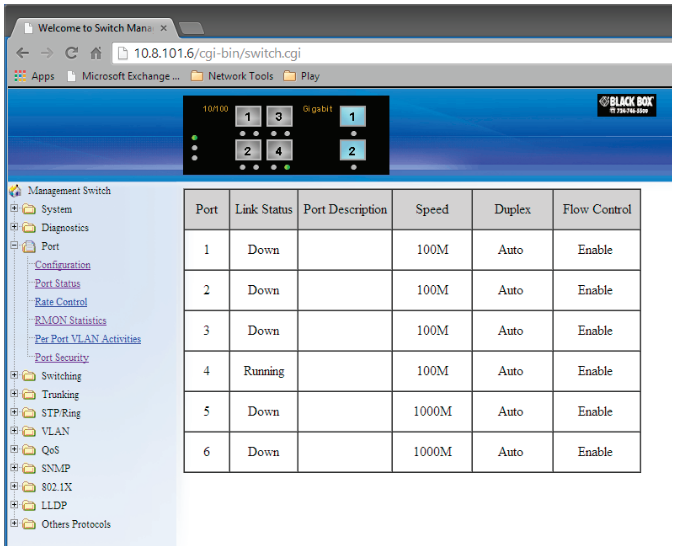
Configuration

1. Port Description: Click in the “Port” text box select the port.
2. Admin Setting: Choose “Link down” or “Link up” from the “Admin Setting” drop-down list to disable or enable Admin Setting for the port.
3. Speed: Click “Speed” drop-d Speed” drop-down list for the port.
4. Flow Control: Click “Flow Co “Flow Control” drop-down list to disable or enable Flow Co
5. Submit: Click “Submit” butto


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
Other b
10/100
Gigabit
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Update Setting

Port	Mode	Add MAC address (Ex:0000.1122.3344)	Delete MAC address
1	Disable		
2	Disable		
3	Disable		
4	Disable		

Note: Port security is not supported on GE ports.

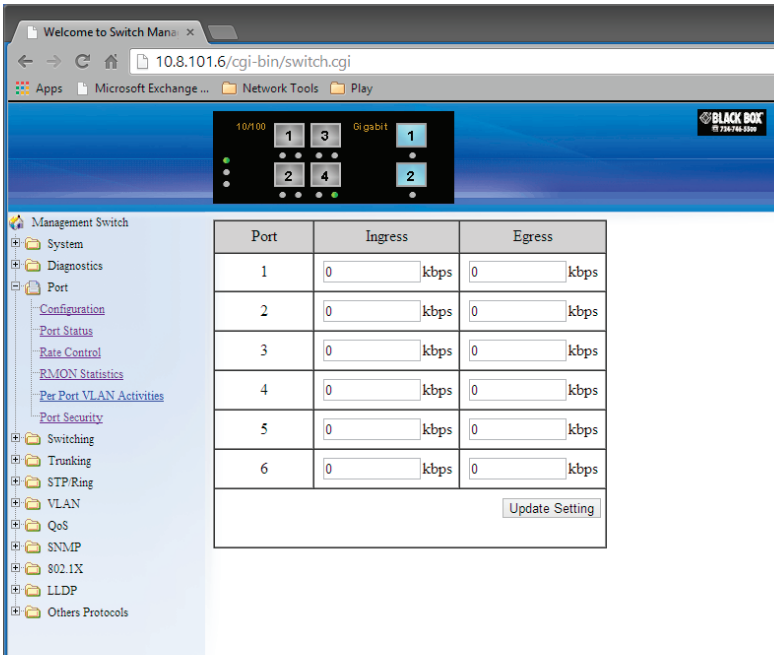

Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols

Port	Link Status	Port Description	Speed	Duplex	Flow Control
1	Down		100M	Auto	Enable
2	Down		100M	Auto	Enable
3	Down		100M	Auto	Enable
4	Running		100M	Auto	Enable
5	Down		1000M	Auto	Enable
6	Down		1000M	Auto	Enable

Figure 6-21. Port status.

Port Status

View the Link Status, Port Description, Speed, Duplex, and Flow Control status for all ports.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Update Setting

Port	Ingress	Egress
1	0 kbps	0 kbps
2	0 kbps	0 kbps
3	0 kbps	0 kbps
4	0 kbps	0 kbps
5	0 kbps	0 kbps
6	0 kbps	0 kbps

Figure 6-22.

Rate Control

1. Ingress: Click in “Ingress” text box and type a new Rate to change the Ingress Rate Control for the port.

Rate Values: 64 kbps, 128 kbps, 192 kbps, … , 1792 kbps.

2 Mbps, 3 Mbps, 4 Mbps, … , 100 Mbps.

104 Mbps, 112 Mbps, 120 Mbps, … , 1000 Mbps.

NOTE: M = 1024k.

2. Egress: Click in “Egress” text box and type a new Rate to change the Egress Rate Control for the port.

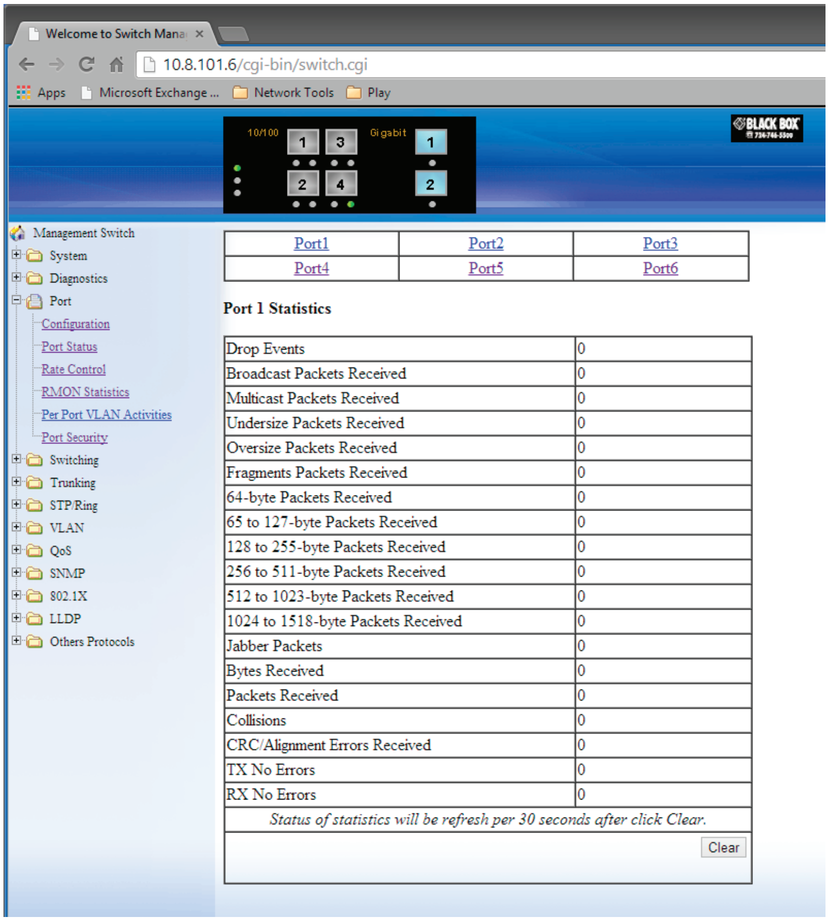
   Rate Values: 64 kbps, 128 kbps, 192 kbps, … , 1792 kbps.

   2 Mbps, 3 Mbps, 4 Mbps, … , 100 Mbps.

   104 Mbps, 112 Mbps, 120 Mbps, … , 1000 Mbps.

NOTE: M = 1024k.

3. Update Setting: Click the “Update Setting” button when you finish these Rate Control settings.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
Gigabit
1
3
2
4
1
2
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Clear

Port1	Port2	Port3
Port4	Port5	Port6

Port 1 Statistics

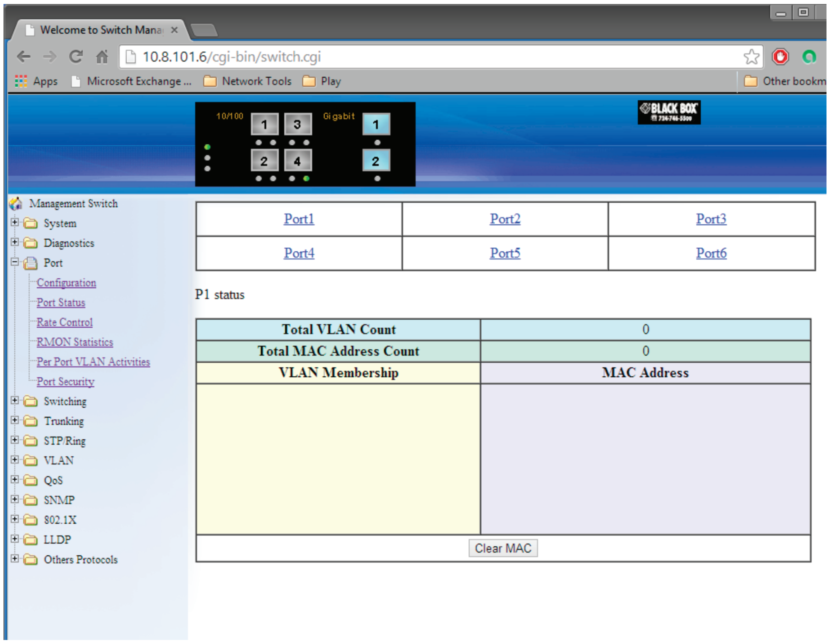
Drop Events	0
Broadcast Packets Received	0
Multicast Packets Received	0
Undersize Packets Received	0
Oversize Packets Received	0
Fragments Packets Received	0
64-byte Packets Received	0
65 to 127-byte Packets Received	0
128 to 255-byte Packets Received	0
256 to 511-byte Packets Received	0
512 to 1023-byte Packets Received	0
1024 to 1518-byte Packets Received	0
Jabber Packets	0
Bytes Received	0
Packets Received	0
Collisions	0
CRC/Alignment Errors Received	0
TX No Errors	0
RX No Errors	0

Status of statistics will be refresh per 30 seconds after click Clear.

Figure 6-23.

RMON Statistics

Click ports to view corresponding RMON Statistics.


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
Other bookm
10/100
Gigabit
BLACK BOX
Management Switch
System
Diagnostics
Port
Configuration
Port Status
Rate Control
RMON Statistics
Per Port VLAN Activities
Port Security
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
802.1X
LLDP
Others Protocols
Clear MAC

Port1	Port2	Port3
Port4	Port5	Port6

P1 status

Total VLAN Count	0
Total MAC Address Count	0
VLAN Membership	MAC Address

Figure 6-24.

Per Port VLAN Activities

Click ports to view corresponding vlan activities.

Port Security

Figure 6-25.

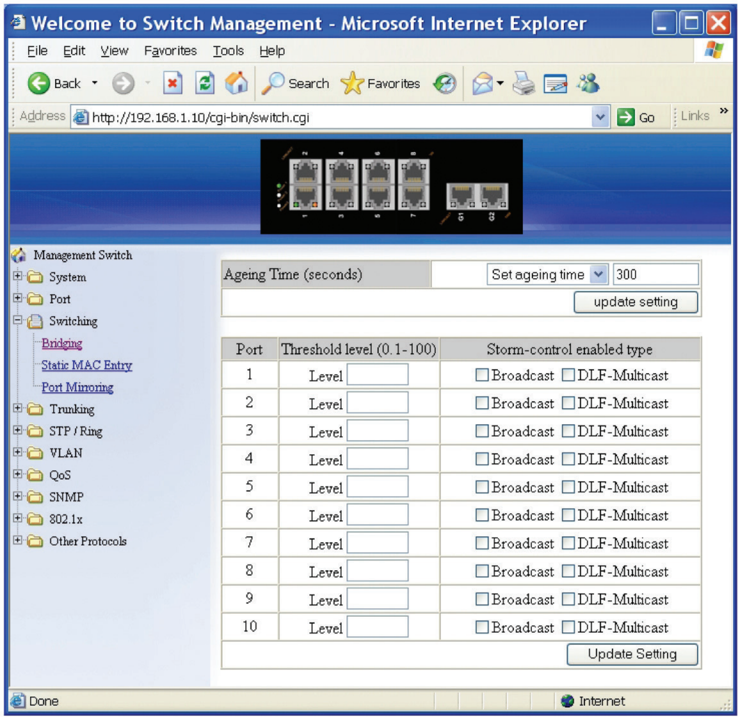
To configure Port Security:

1. Click on Port/Port Security from the Left navigation window.
2. Select “enable” from the drop-down list next to the port number of the port that you want the Port Security to be configured.

3. In the “Add MAC Address” text entry box for each port, enter the MAC address of the device that you want to allow access to on this port. You can configure up to 24 MAC address for each port.

Click on the “Update Setting” button to activate the new configuration

6.6 Switching


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Bridging
Static MAC Entry
Port Mirroring
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
update setting
Update Setting
Done
Internet

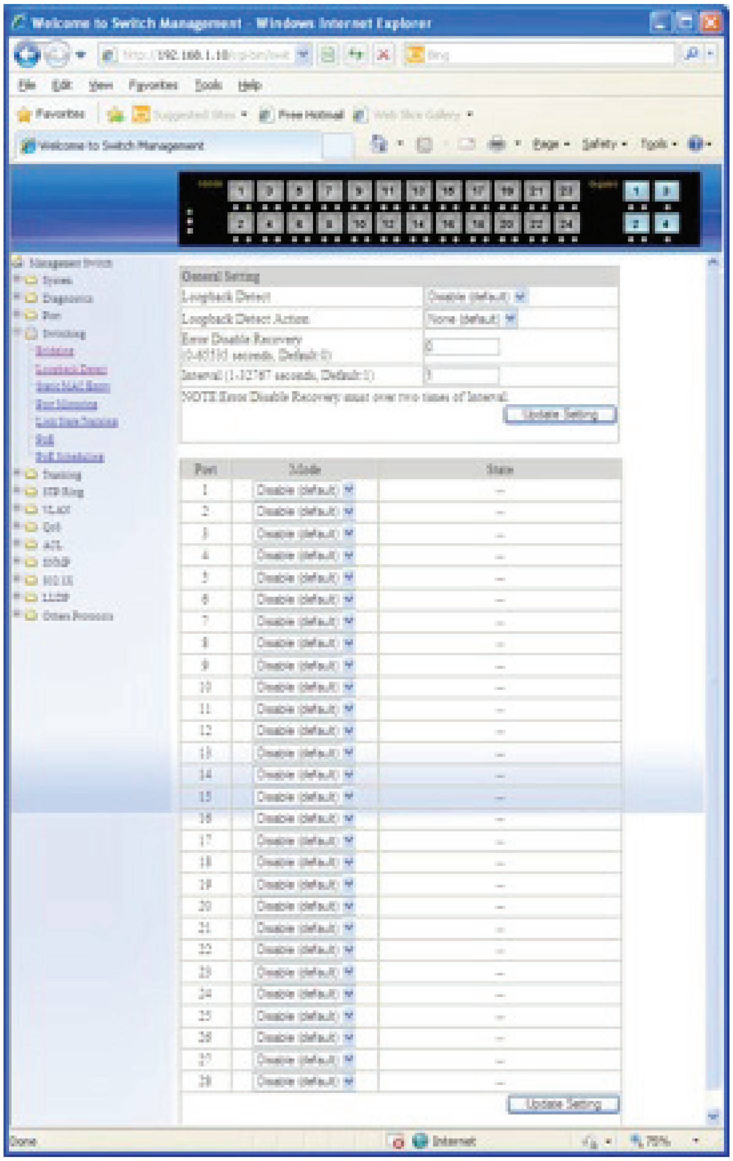
Ageing Time (seconds) Set ageing time 300

Port	Threshold level (0.1-100)	Storm-control enabled type
1	Level	☐ Broadcast ☐ DLF-Multicast
2	Level	☐ Broadcast ☐ DLF-Multicast
3	Level	☐ Broadcast ☐ DLF-Multicast
4	Level	☐ Broadcast ☐ DLF-Multicast
5	Level	☐ Broadcast ☐ DLF-Multicast
6	Level	☐ Broadcast ☐ DLF-Multicast
7	Level	☐ Broadcast ☐ DLF-Multicast
8	Level	☐ Broadcast ☐ DLF-Multicast
9	Level	☐ Broadcast ☐ DLF-Multicast
10	Level	☐ Broadcast ☐ DLF-Multicast

Figure 6-26.

Bridging

1. Aging Time (seconds): Click the text box and type a decimal number as Bridging Aging Time in seconds.
2. Update Setting: Click on the “Update Setting” button when you finish configuring Aging Time.
3. Threshold Level (0.1–100): Click in the “Level” text box and type a decimal number for the port. You need to choose “Broadcast” and/or “DFL-Multicast“ “Storm-control enabled type” for the port. DLF (Destination Lookup Failure).
4. Storm Control Enabled Type: Choose “Broadcast” and/or “DLF-Multicast” from “Storm-control enabled type” for the port.
5. Port Isolation: Choose “Enable” or “Disable” from the “Port Isolation” drop-down list to enable or disable port isolation for the port.
6. Update Setting: Click “Update Setting” button when you finish Threshold Level, Storm Control Enabled Type, and Port Isolation settings.



General Setting

Loopback Detect	Disable (default)
Loopback Detect Action	None (default)
Error Disable Recovery (0-65535 seconds, Default 0)	0
Interval (1-32767 seconds, Default 1)	1

NOTE:Error Disable Recovery must over two times of Interval.

Port	Mode	State
1	Disable (default)	--
2	Disable (default)	--
3	Disable (default)	--
4	Disable (default)	--
5	Disable (default)	--
6	Disable (default)	--
7	Disable (default)	--
8	Disable (default)	--
9	Disable (default)	--
10	Disable (default)	--
11	Disable (default)	--
12	Disable (default)	--
13	Disable (default)	--
14	Disable (default)	--
15	Disable (default)	--
16	Disable (default)	--
17	Disable (default)	--
18	Disable (default)	--
19	Disable (default)	--
20	Disable (default)	--
21	Disable (default)	--
22	Disable (default)	--
23	Disable (default)	--
24	Disable (default)	--
25	Disable (default)	--
26	Disable (default)	--
27	Disable (default)	--
28	Disable (default)	--

FIgure 6-27.

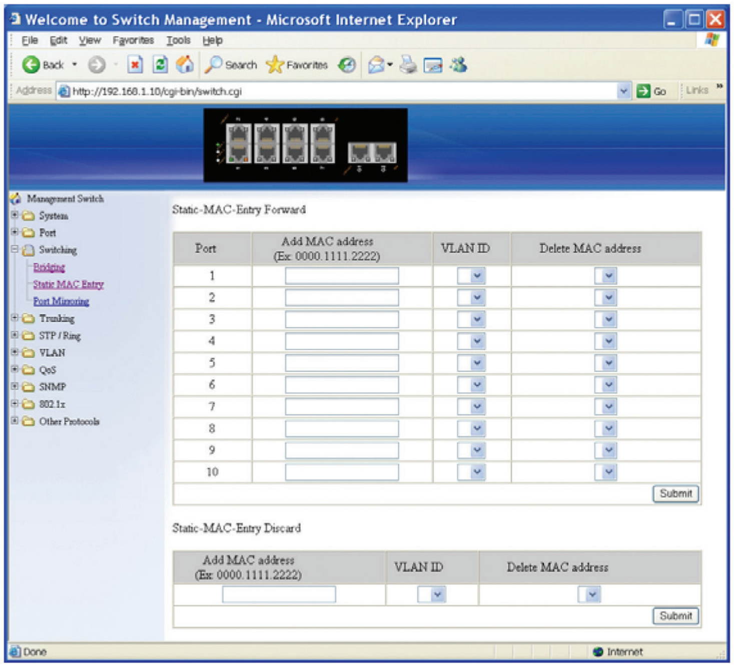
Loopback Detect

General Setting:

1. Detect: Choose "Disable (default)" or "Enable" from the "Detect" drop-down list to disable or enable a loopback detection on a port interface.
2. Detect Action: Choose "None (default)" or "Error Disable" from "Detect Action" drop-down list to disable or enable error disable Detect Action on a port interface.
3. Error Disable Recovery (0–65535 seconds): Click the text box and type a decimal number for the error disable recovery time in seconds. The default value is 0 second (no recovery).
4. Interval (1–65535 seconds): Click the text box and type a decimal number for the loopback detect interval time in seconds. The default value is 1 second.
5. Update Setting: Click "Update Setting" button when you finish General Setting.

For Port Interface:

1. Mode: Choose "Enable" or "Disable (default)" from the "Mode" drop-down list to enable or disable Detect for a port interface.
2. Update Setting: Click the "Update Setting" button when you finish the Detect settings for port interface.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Bridging
Static MAC Entry
Port Mirroring
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
Submit
Submit
Done
Internet

Static-MAC-Entry Forward

Port	Add MAC address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Static-MAC-Entry Discard

Add MAC address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC address

FIgure 6-28. Static MAC entry.

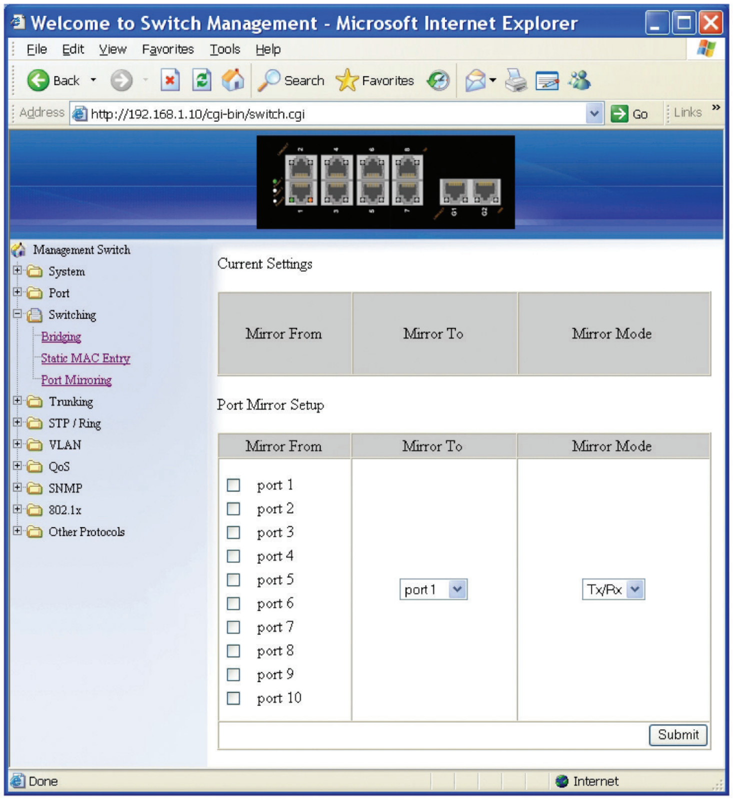
Static MAC Entry

Static-MAC-Entry Forward:

1. Add MAC Address: Click in the "Add MAC Address" text box and type a locked forwarding MAC address for the port.
2. VLAN ID: Click on the "VLAN ID" drop-down menu and choose a VLAN ID from the "VLAN ID" drop-down list.
3. Delete MAC Address: Click on the "Delete MAC Address" drop-down menu and choose a locked forwarding MAC address from the "Delete MAC Address" drop-down list to be deleted from the port.
4. Submit: Click on the "Submit" button when you finish Static-MAC-Entry Forward settings.

Static-MAC-Entry Discard:

1. Add MAC Address: Click in the "Add MAC Address" text box and type a MAC address to be discarded for the VLAN.
2. VLAN ID: VLAN ID: Choose a VLAN ID from the "VLAN ID" drop-down list.
3. Delete MAC Address: Choose a MAC address from the "Delete MAC Address" drop-down list to be discarded from the VLAN.
4. Submit: Click on the "Submit" button when you finish Static-MAC-Entry Discard settings.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Management Switch
System
Port
Switching
Bridging
Static MAC Entry
Port Mirroring
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
Submit
Done
Internet

http://192.168.1.10/cgi-bin/switch.cgi

Current Settings

Mirror From	Mirror To	Mirror Mode

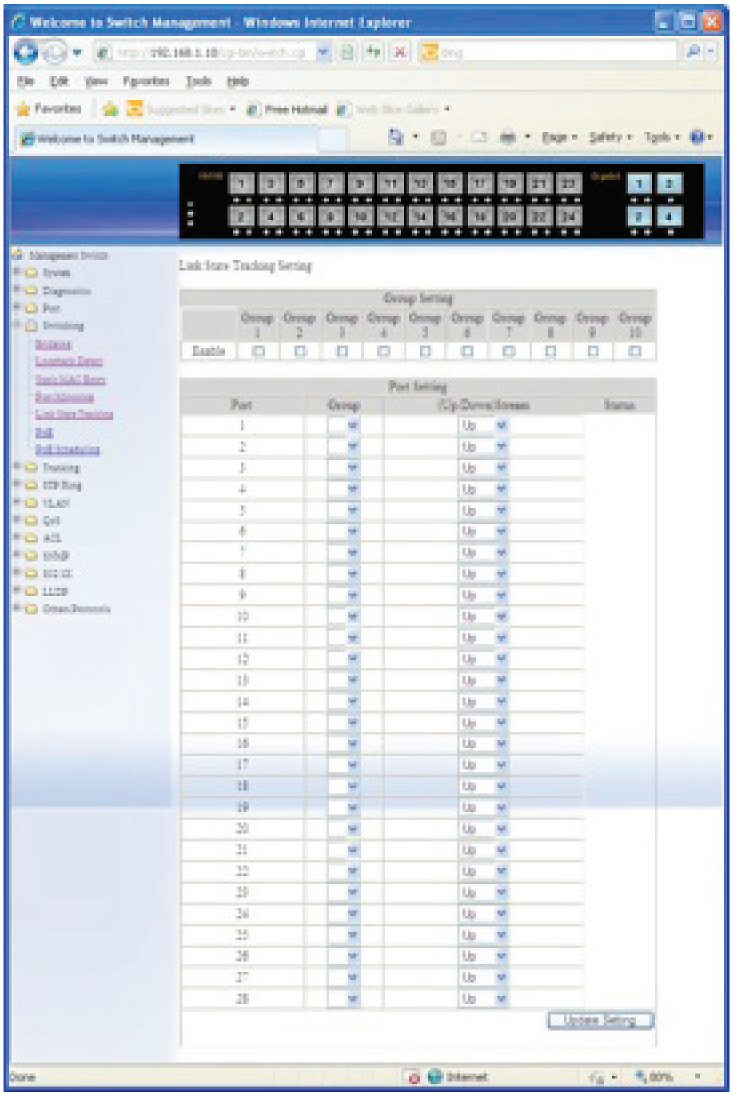
Port Mirror Setup

Mirror From	Mirror To	Mirror Mode
☐ port 1 ☐ port 2 ☐ port 3 ☐ port 4 ☐ port 5 ☐ port 6 ☐ port 7 ☐ port 8 ☐ port 9 ☐ port 10	port 1	Tx/Rx

Figure 6-29.

Port Mirroring

1. Mirror From: Choose Mirror From port from Port 1–Port 28.
2. Mirror To: Click “Mirror To” drop-down menu to choose Mirror To port (Port 1–Port 28) from “Mirror To” drop-down list.
3. Mirror Mode: Click “Mirror Mode” drop-down menu to choose “Tx/Rx”, “Tx”, or “Rx” from “Mirror Mode” drop-down list.
4. Submit: Click “Submit” button when you finish Port Mirroring settings.



Link State Tracking Setting

Group Setting										
	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Group 8	Group 9	Group 10
Enable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Port Setting			
Port	Group	(Up/Down)Stream	Status
1		Up	
2		Up	
3		Up	
4		Up	
5		Up	
6		Up	
7		Up	
8		Up	
9		Up	
10		Up	
11		Up	
12		Up	
13		Up	
14		Up	
15		Up	
16		Up	
17		Up	
18		Up	
19		Up	
20		Up	
21		Up	
22		Up	
23		Up	
24		Up	
25		Up	
26		Up	
27		Up	
28		Up	

Figure 6-30.

Link State Tracking

Group Setting:

1. Enable: Click the check box of a group to enable Link State tracking for a group.

Port Setting:

1. Group: Click the "Group" drop-down menu to choose a group for port from the "Group" drop-down list.
2. (Up/Down)Stream: Click "(Up/Down)Stream" drop-down menu to choose Up (upstream) or Down (downstream) for a port from "(Up/Down)Stream" drop-down list.
3. Update Setting: Click on the "Update Setting" button when you finish Link State Tracking Setting.

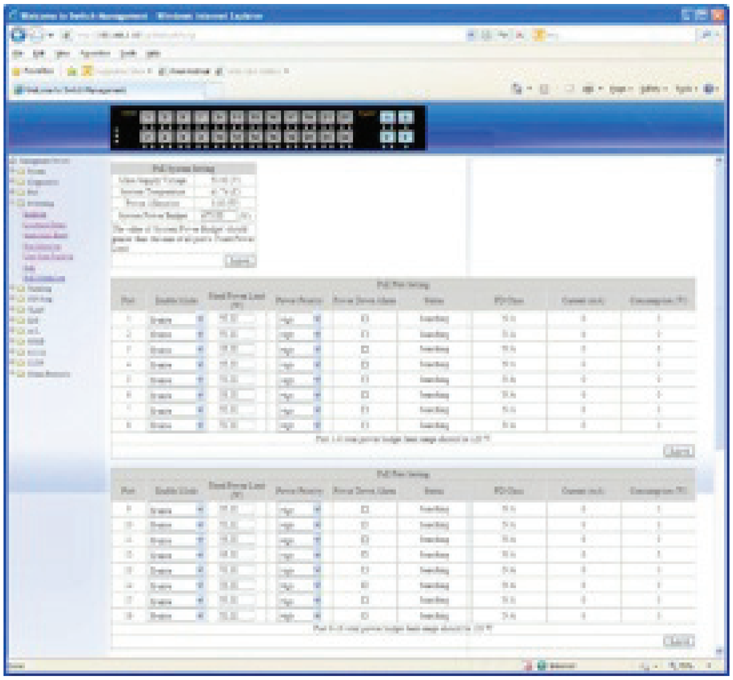


Figure 6-31.

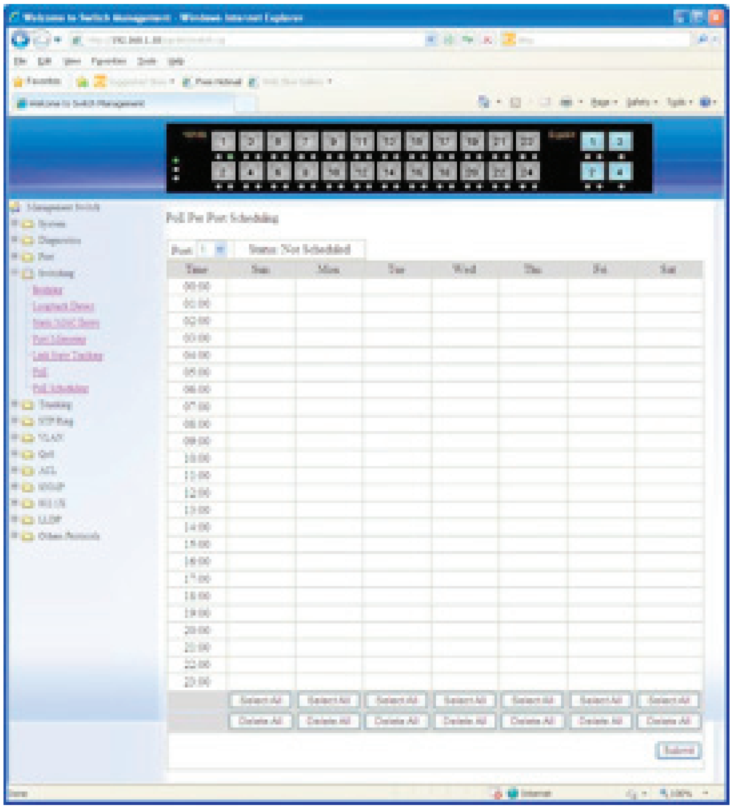
PoE (for LEH1000 Series switches only)

PoE System Setting:

1. System Power Budget: Click in the "System Power Budget" text box and type a new system power budget for the switch.
2. Submit: Click on the "Submit" button when you finish PoE System Setting.

PoE Port Setting:

1. Enable Mode: Choose "Disable" or "Enable" from "Enable Mode" drop-down list to disable or enable this port to discover the Powered Device (PD) connected to this port.
2. Fixed Power Limit (W): First uncheck "Power Limit by Classification" to disable this port to provide power to PD according to classification of maximum power range used by the PD. Then click in "Fixed Power Limit (W)" text box and type a new fixed power limit for this port to provide power to the PD.
3. Power Priority: Choose "High", "Medium", or "Low" from the "Power Priority" drop-down list to determine power priority of this port.
4. Power Down Alarm: Check or uncheck "Power Down Alarm" to enable or disable power down alarm on this port.
5. Submit: Click on the "Submit" button when you finish the PoE Port Setting.


PoE Per Port Scheduling

Port: 1 Status: Not Scheduled

Time
Sun
Mon
Tue
Wed
Thu
Fri
Sat
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
Select All
Delete All
Submit

Figure 6-32.

PoE Scheduling (for LEH1000 Series switches only)

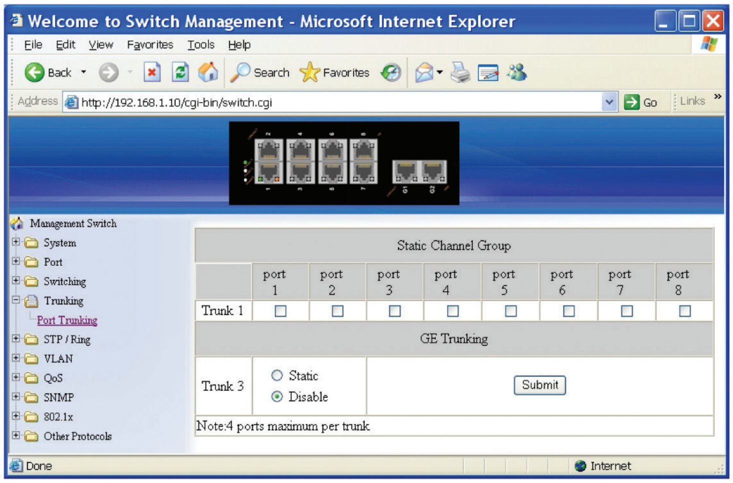
First click on “Switching” from the main menu. Then click on “PoE” from “Switching.” In the PoE Port Setting, choose “Scheduling” from the “Enable Mode” drop-down list to schedule this port to discover the Powered Device (PD) connected to this port.

PoE Per Port Setting:

1. Port: Click on the “Port” drop-down menu to choose a port from the “Port” drop-down list and configure PoE scheduling to this port.

2. Submit: Click on the “Submit” button when you finish PoE Scheduling for this port.

6.7 Trunking


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
Port Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

Static Channel Group

	port 1	port 2	port 3	port 4	port 5	port 6	port 7	port 8
Trunk 1	☐	☐	☐	☐	☐	☐	☐	☐

GE Trunking

Trunk 3: ○ Static ● Disable

Submit

Note:4 ports maximum per trunk

FIgure 6-33.

Port Trunking

Static Channel Group:

1. Trunk 1: Click ports to assign ports to Trunk 1. (Maximum 4 ports per Trunk.)

LACP Group:

1. Trunk 1: Click ports to assign ports to Trunk 1. (Maximum 4 ports in Trunk 1.)

GE Trunking (Gigabit Ports):

1. Trunk 3: Check "Static," "LACP," or "Disable" to enable Static or LACP Trunk 3 or disable Trunk 3 for Gigabit Ethernet ports.

Submit: Click on the "Submit" button when you finish Port Trunking settings.

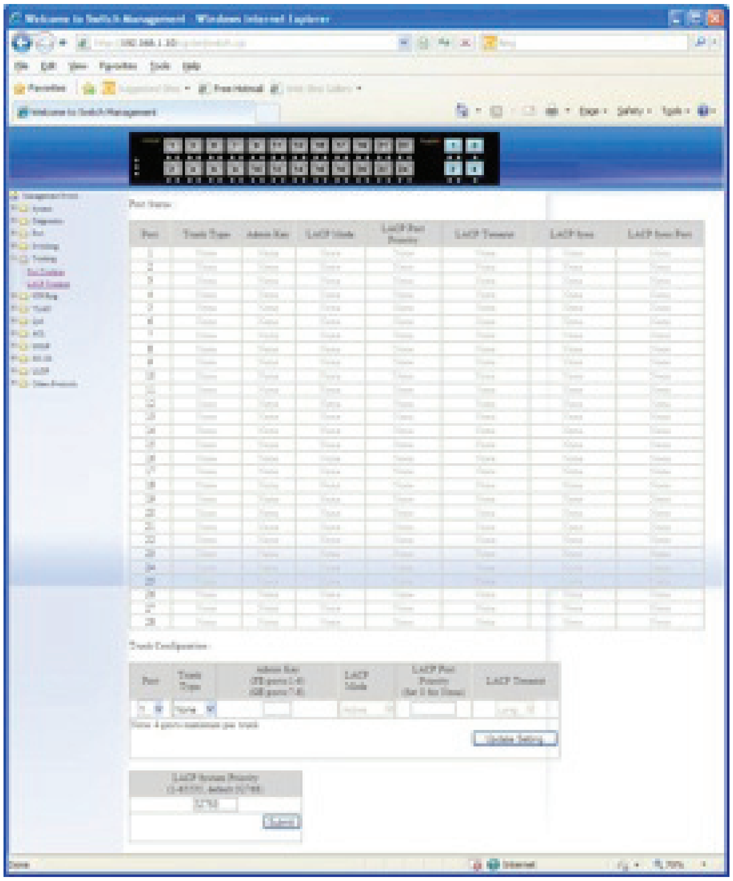


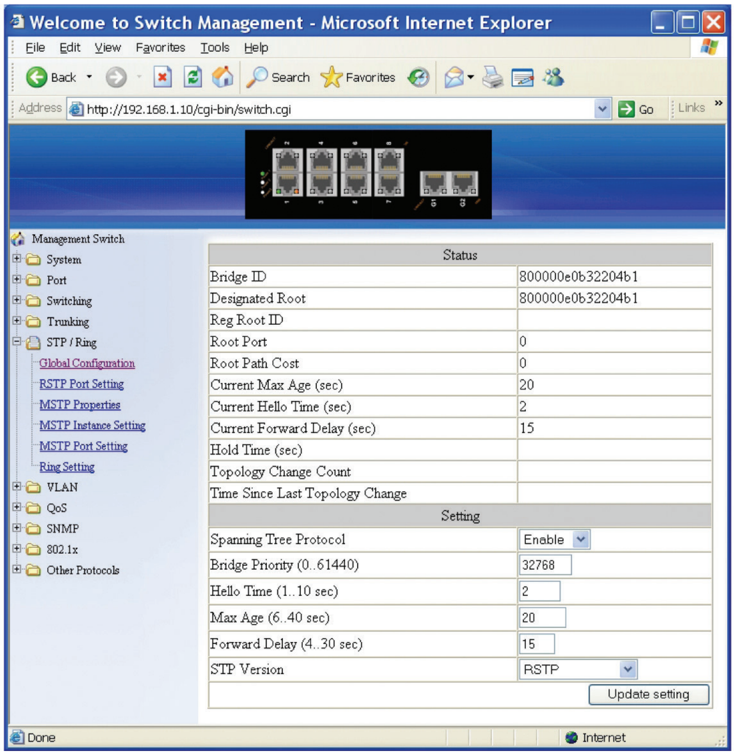
Figure 6-34.

LACP Trunking

Trunk Configuration:

1. Port: Choose a port from the “Port” drop-down list.
2. Trunk Type: Choose “None,” “Static,” or “LACP” from the “Trunk Type” drop-down list to disable or enable Static or LACP Trunk.
3. Admin Key: Click in “Admin Key” text box and type a decimal number 1–6 for FE ports. Type a decimal number 7–8 for GE ports.
4. LACP Mode: Choose “Active” or “Passive” from the “LACP Mode” drop-down list to enable Active or Passive LACP Mode.
5. LACP Port Priority (Set 0 for None): Click in the “LACP Port Priority” text box and type 1–65535 for the port. The default value is 32768.
6. LACP Timeout: Choose “Long” or “Short” from the “LACP Timeout” drop-down list to enable Long or Short LACP Timeout. The long timeout value is 90 seconds. The short timeout value is 3 seconds.
7. Update Setting: Click on the “Update Setting” button when you finish Trunk Configuration.
8. LACP System Priority (1-65535, default 32768): Click in “LACP System Priority” text box and type 1-65535. Default value is 32768.
9. Submit: Click on the “Submit” button when you finish LACP System Priority settings.

6.8 STP/Ring

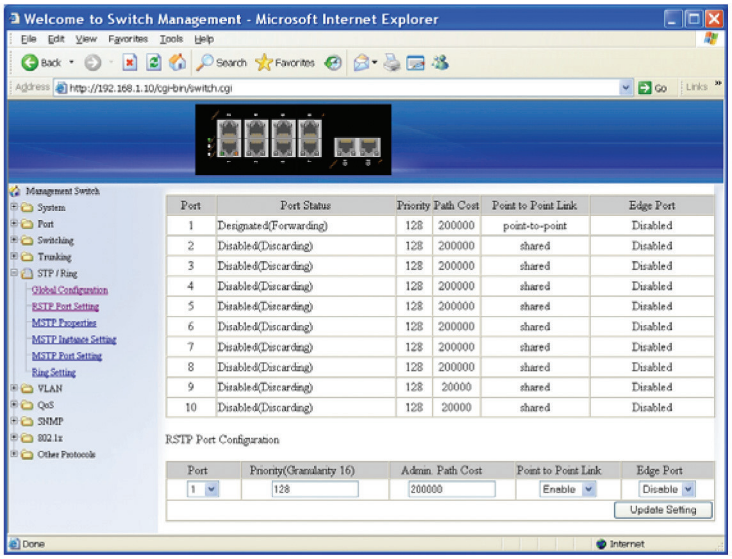

Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

Status	
Bridge ID	800000e0b32204b1
Designated Root	800000e0b32204b1
Reg Root ID	
Root Port	0
Root Path Cost	0
Current Max Age (sec)	20
Current Hello Time (sec)	2
Current Forward Delay (sec)	15
Hold Time (sec)	
Topology Change Count	
Time Since Last Topology Change	
Setting	
Spanning Tree Protocol	Enable
Bridge Priority (0..61440)	32768
Hello Time (1..10 sec)	2
Max Age (6..40 sec)	20
Forward Delay (4..30 sec)	15
STP Version	RSTP
	Update setting

Figure 6-35.

Global Configuration

1. Spanning Tree Protocol: Choose "Enable" or "Disable" from "Spanning Tree Protocol" drop-down list to enable or disable Spanning Tree Protocol.
2. Bridge Priority (0..61440): Click in the "Bridge Priority" text box and type a decimal number between 0 and 61440.
3. Hello Time (sec) (1..9 sec): Click in the "Hello Time" text box and type a decimal number between 1 and 9.
4. Max Age (sec) (6..28 sec): Click in the"Max Age" text box and type a decimal number between 6 and 28.
5. Forward Delay (sec) (4..30 sec): Click in the "Forward Delay" text box and type a decimal number between 4 and 30.
6. STP Version: Choose "MSTP", "RSTP" or "STP compatible" from "STP Version" drop-down list.
7. Update Setting: Click the "Update Setting" button when you finish Global Configuration.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Update Setting
Done
Internet

Port	Port Status	Priority	Path Cost	Point to Point Link	Edge Port
1	Designated(Forwarding)	128	200000	point-to-point	Disabled
2	Disabled(Discarding)	128	200000	shared	Disabled
3	Disabled(Discarding)	128	200000	shared	Disabled
4	Disabled(Discarding)	128	200000	shared	Disabled
5	Disabled(Discarding)	128	200000	shared	Disabled
6	Disabled(Discarding)	128	200000	shared	Disabled
7	Disabled(Discarding)	128	200000	shared	Disabled
8	Disabled(Discarding)	128	200000	shared	Disabled
9	Disabled(Discarding)	128	20000	shared	Disabled
10	Disabled(Discarding)	128	20000	shared	Disabled

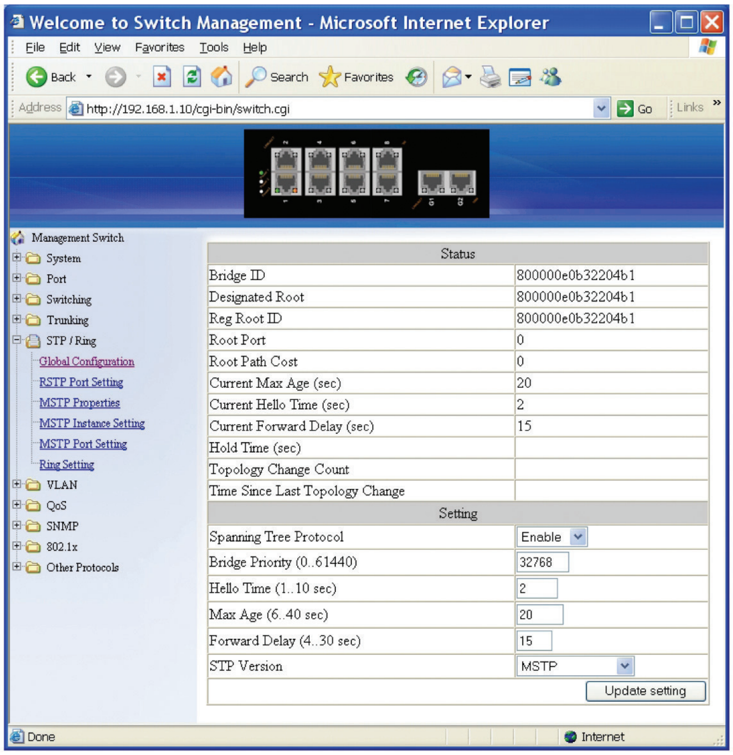
RSTP Port Configuration

Port	Priority(Granularity 16)	Admin. Path Cost	Point to Point Link	Edge Port
1	128	200000	Enable	Disable

Figure 6-36.

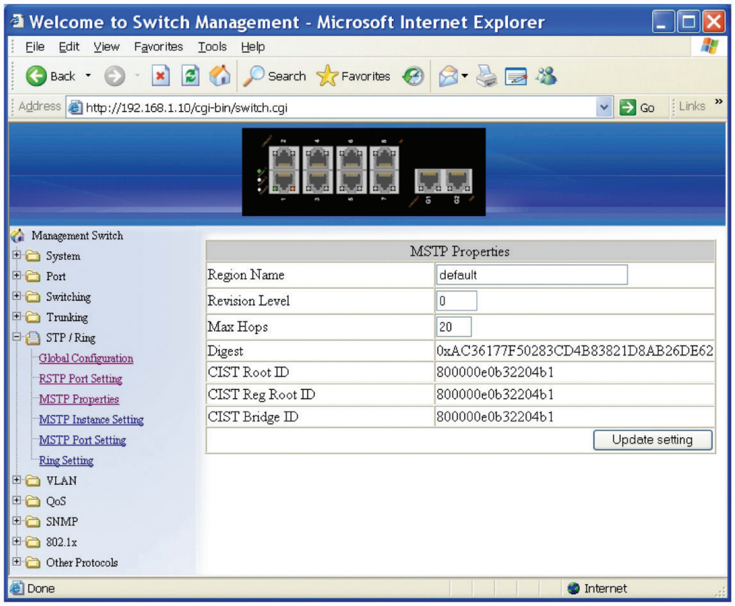
RSTP Port Setting

1. STP Version: Choose "RSTP" from the "STP Version" drop-down list.
2. Port: Choose a port from "Port" drop-down list.
3. Priority(Granularity 16): Click in the "Priority" text box and enter a value between 0 and 240 to set the priority for the port. A higher priority will designate the port to forward packets first. A lower number denotes a higher priority. This entry must be divisible by 16. The default priority setting is 128.
4. Admin. Path Cost: Click in the "Admin. Path Cost" text box and enter a value between 0 and 2000000 to set the Admin. Path Cost for the port. 0 (auto) - Setting 0 for the Admin. Path Cost will automatically set the speed for forwarding packets to the port for optimal efficiency. The default port cost: 100 Mbps port = 200000. Gigabit port = 20000.
5. Point to Point Link: Choose "Enable" or "Disable" from "Point to Point Link" drop-down list to enable or disable Point to Point Link for the port.
6. Edge Port: Choose "Enable", "Disable", or "Auto" from "Edge Port" drop-down list to set Enable, Disable, or Auto Edge Port for the port.
7. Update Setting: Click on the "Update Setting" button when you finish RSTP Port Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Update setting
Done
Internet

Status	
Bridge ID	800000e0b32204b1
Designated Root	800000e0b32204b1
Reg Root ID	800000e0b32204b1
Root Port	0
Root Path Cost	0
Current Max Age (sec)	20
Current Hello Time (sec)	2
Current Forward Delay (sec)	15
Hold Time (sec)	
Topology Change Count	
Time Since Last Topology Change	
Setting	
Spanning Tree Protocol	Enable
Bridge Priority (0..61440)	32768
Hello Time (1..10 sec)	2
Max Age (6..40 sec)	20
Forward Delay (4..30 sec)	15
STP Version	MSTP

FIgure 6-37.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Update setting
Done
Internet

MSTP Properties	
Region Name	default
Revision Level	0
Max Hops	20
Digest	0xAC36177F50283CD4B83821D8AB26DE62
CIST Root ID	800000e0b32204b1
CIST Reg Root ID	800000e0b32204b1
CIST Bridge ID	800000e0b32204b1

Figure 6-38.

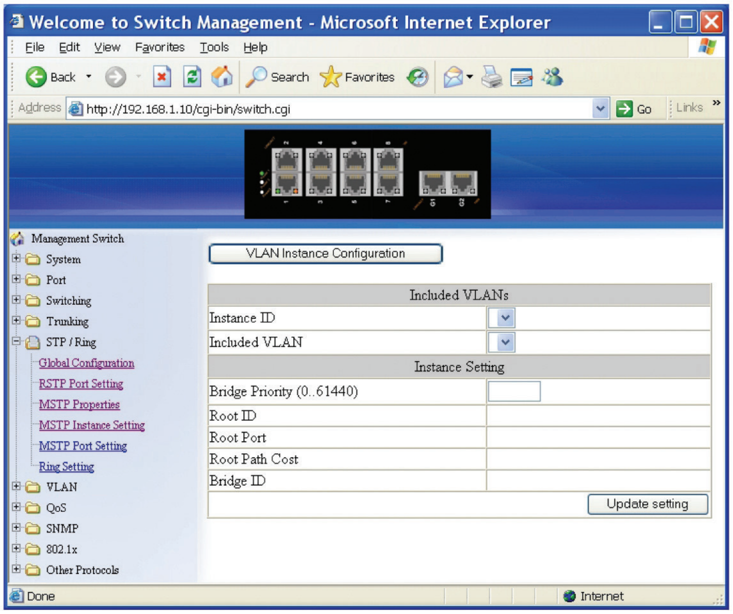
MSTP Properties

1. STP Version: Choose “MSTP” from “STP Version” drop-down list.
2. Region Name: Click in the “Region Name” text box to create an MST region and specify a name for it. MST bridges of a region form different spanning trees for different VLANs. By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

3. Revision Level: Click in the “Revision Level” text box to specify the number for configuration information. The default value of| revision number is 0.

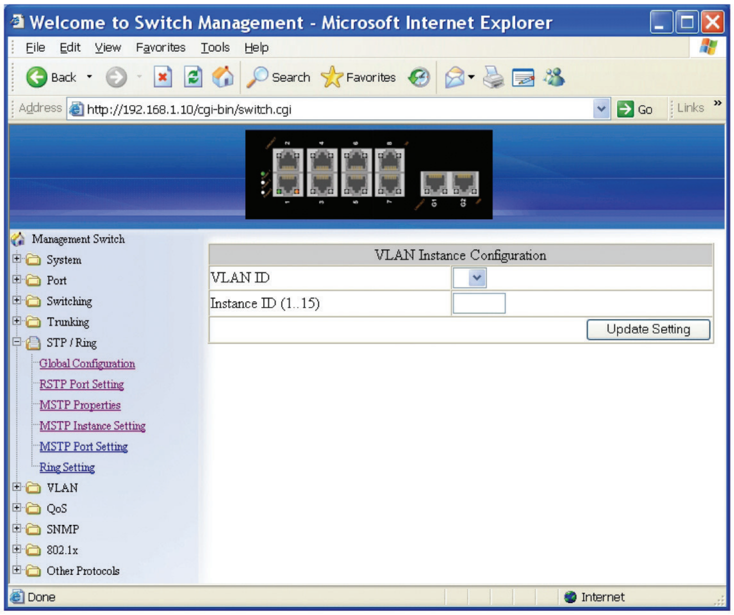
4. Max Hops: Click in the “Max Hops” text box to specify the maximum allowed hops for BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the max hops for a BPDU prevents the messages from looping indefinetely in the network. When a bridge receives a MST BPDU that has exceeded the allowed max-hops, it discards the BPDU.

5. Update Setting: Click on the “Update Setting” button when you finish MSTP Properties setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
VLAN Instance Configuration
Update setting
Done
Internet

Included VLANs	
Instance ID	
Included VLAN	
Instance Setting	
Bridge Priority (0..61440)	
Root ID	
Root Port	
Root Path Cost	
Bridge ID	

Figure 6-39.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Update Setting
Done
Internet

VLAN Instance Configuration	
VLAN ID	
Instance ID (1..15)	

Figure 6-40.

MSTP Instance Setting

VLAN Instance Configuration:

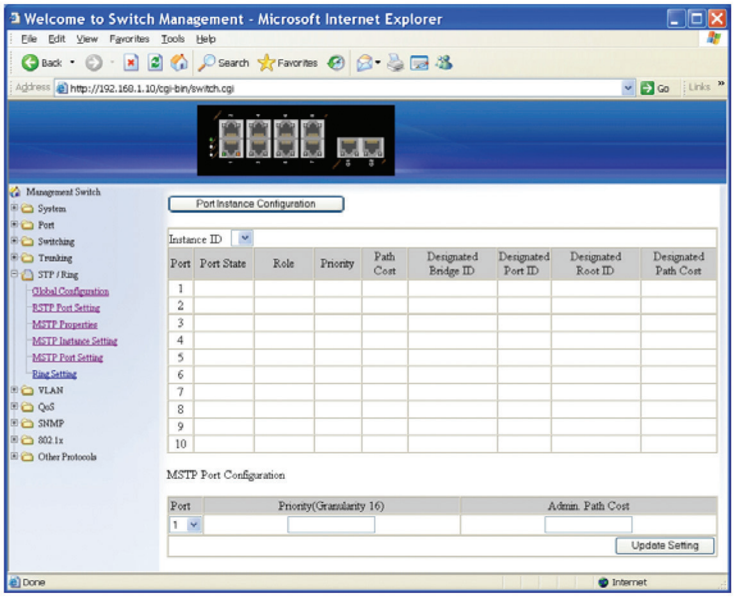
1. VLAN Instance Configuration: Click on the "VLAN Instance Configuration" button. The "VLAN Instance Configuration" window appears.
2. VLAN ID: Choose VLAN from the "VLAN ID" drop-down list to simultaneously add multiple VLANs for the corresponding instance of a bridge.
3. Instance ID (1..15): Click in "Instance ID" text box to specify the instance ID.
4. Update Setting: Click on the "Update Setting" button when you finish VLAN Instance Configuration.

Included VLANs:

1. Instance ID: Click on the "Instance ID" drop-down menu to choose instance ID from "Instance ID" drop-down list.
2. Included VLAN: Choose a VLAN from "Included VLAN" drop-down list.

Instance Setting:

1. Bridge Priority (0..61440): Click in "Bridge Priority" text box to set the bridge priority for an MST instance to the value specified. The lower the priority of the bridge, the better the chances are that the bridge will become a root bridge or a designated bridge for the LAN.
2. Update Setting: Click "Update Setting" button when you finish VLAN Instance Configuration.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Port Instance Configuration
Update Setting
Done
Internet

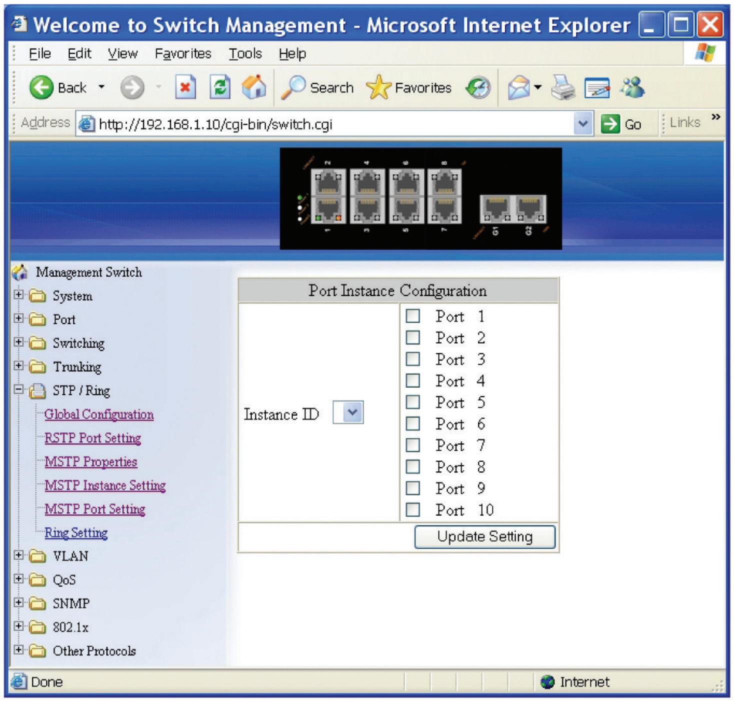
Instance ID

Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	Designated Path Cost
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

MSTP Port Configuration

Port	Priority(Granularity 16)	Admin. Path Cost
1		

FIgure 6-41.



Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

Port Instance Configuration

Instance ID	☐ Port 1 ☐ Port 2 ☐ Port 3 ☐ Port 4 ☐ Port 5 ☐ Port 6 ☐ Port 7 ☐ Port 8 ☐ Port 9 ☐ Port 10
	Update Setting

Figure 6-42.

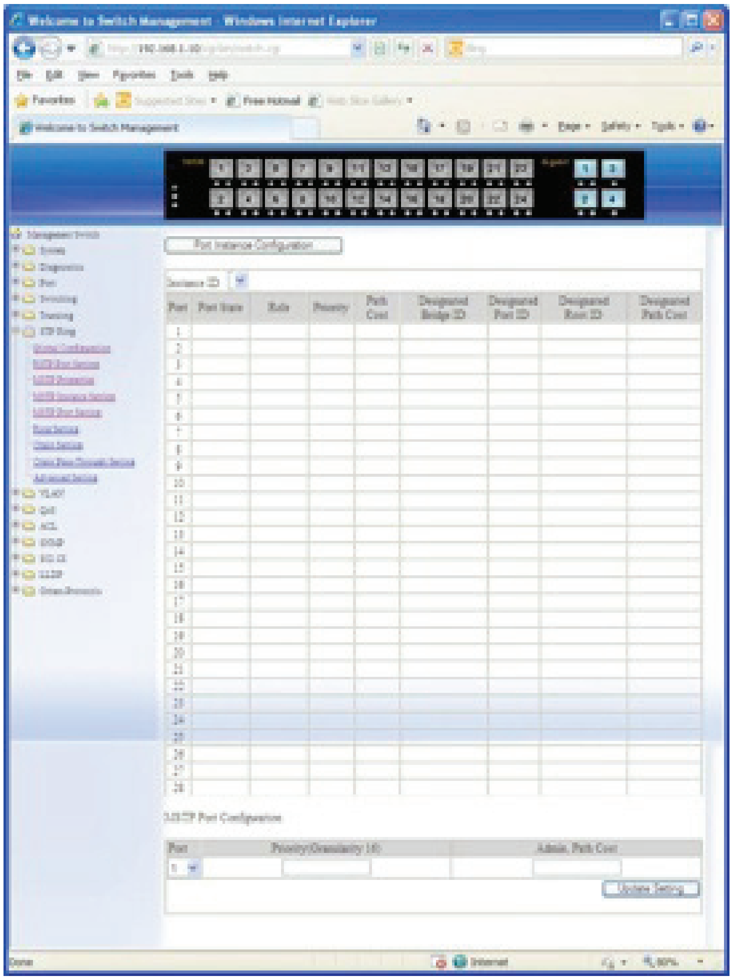

Port Instance Configuration
Instance ID
Port
Port State
Role
Priority
Path Cost
Designated Bridge ID
Designated Port ID
Designated Root ID
Designated Path Cost
MSTP Port Configuration
Priority(Granularity 16)
Admin. Path Cost
Update Setting

Figure 6-43.

MSTP Port Setting

Port Instance Configuration

1. Instance ID: Click on the "Instance ID" drop-down menu to choose instance ID from the "Instance ID" drop-down list.
2. Click ports to assign ports to the corresponding instance ID.
3. Update Setting: Click the "Update Setting" button when you finish Port Instance Configuration.

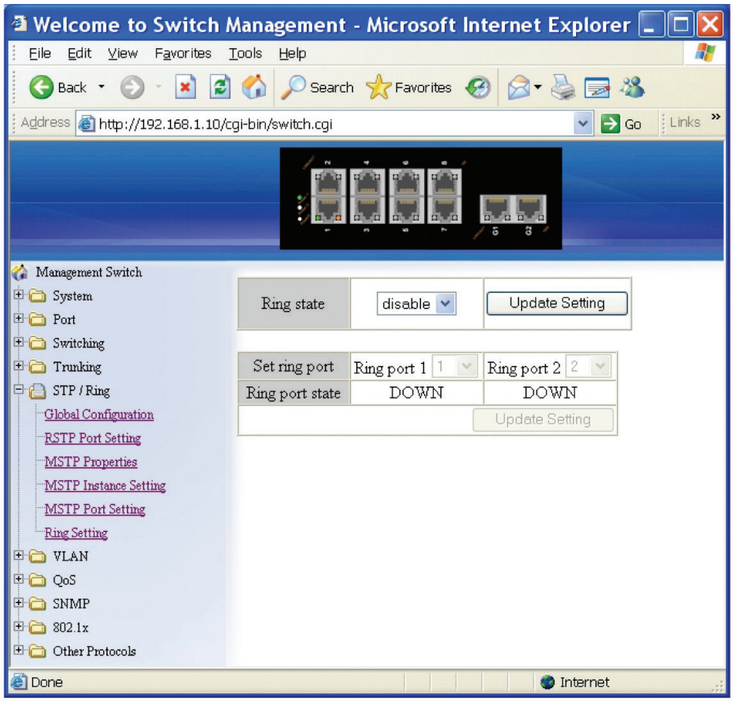
Instance ID

1. Instance ID: Choose instance ID from "Instance ID" drop-down list.

MSTP Port Configuration

1. Port: Choose a port from the "Port" drop-down list.
2. Priority (Granularity 16): Click in the "Priority" text box to set the port priority for a bridge group. The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others. The permitted range is 0–240. The priority values can only be set in increments of 16.
3. Admin. Path Cost: Click in the "Admin. Path Cost" text box to set the cost of a path associated with an interface.

4. Update Setting: Click on the “Update Setting” button when you finish MSTP Port Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

Ring state	disable	Update Setting

Set ring port	Ring port 1 1	Ring port 2 2
Ring port state	DOWN	DOWN
		Update Setting

Figure 6-44.

Ring Setting

Ring State:

1. Click on the “Ring State” drop-down menu from the “Ring State” drop-down list to choose “Enable” or “Disable” to enable or disable Ring State.

2. Update Setting: Click on the “Update Setting” button when you finish the Ring State setting.

Set Ring Port:

1. Ring Port 1: Choose Ring Port 1 from the “Ring Port 1” drop-down list.

2. Ring Port 2: Choose Ring Port 2 from the “Ring Port 2” drop-down list.

3. Update Setting: Click on the“Update Setting” button when you finish Set Ring Port.

Ring Coupling State:

1. Choose “Enable” or “Disable” to enable or disable Ring Coupling State.

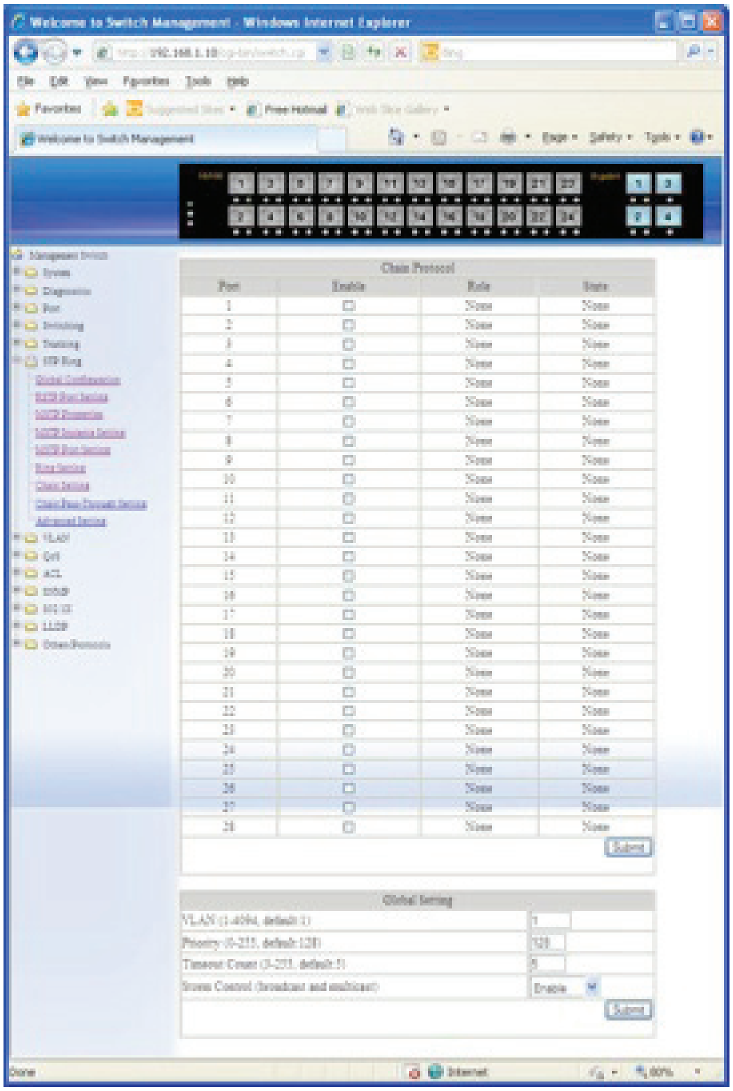
2. Update Setting: Click on the “Update Setting” button when you finish Ring Coupling State setting.

Set Ring Coupling Port:

1. Ring Coupling Port 1: Choose Ring Coupling Port 1 from the “Ring Coupling Port 1” drop-down list.

2. Ring Coupling Port 2: Choose Ring Coupling Port 2 from tyhe “Ring Coupling Port 2” drop-down list.

3. Update Setting: Click on the “Update Setting” button when you finish Set Ring Coupling Port.



Chain Protocol

Port	Enable	Role	State
1	☐	None	None
2	☐	None	None
3	☐	None	None
4	☐	None	None
5	☐	None	None
6	☐	None	None
7	☐	None	None
8	☐	None	None
9	☐	None	None
10	☐	None	None
11	☐	None	None
12	☐	None	None
13	☐	None	None
14	☐	None	None
15	☐	None	None
16	☐	None	None
17	☐	None	None
18	☐	None	None
19	☐	None	None
20	☐	None	None
21	☐	None	None
22	☐	None	None
23	☐	None	None
24	☐	None	None
25	☐	None	None
26	☐	None	None
27	☐	None	None
28	☐	None	None

Global Setting

VLAN (1-4094, default:1)	1
Priority (0-255, default:128)	128
Timeout Count (3-255, default:5)	5
Storm Control (broadcast and multicast)	Enable

Welcome to Switch Management - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
Submit
Submit
Done
Internet

Figure 6-45.

Chain Setting

Chain Protocol:

1. Click “Enable” to enable Chain Protocol for ports.

2. Submit: Click on the “Submit” button when you finish Chain Protocol setting.

Global Setting:

1. VLAN (1-4094, default: 1): Click in the “VLAN” textbox and specify a VLAN ID number from 1–4094.

2. Priority (1-255, default: 128): Set the Switch priority for a running chain protocol. A switch with lower priority will run as the Master (forwarding) port.

3. Timeout Count (3-255, default: 5): Set the Switch timeout count for running chain protocol.

   Chain recovery time = (Chain Timeout Count – 1) x 200 ms.

   Default Chain recovery time = (5 – 1) x 200 ms = 800 ms.

4. Storm Control (broadcast and multicast): Choose “Enable” or “Disable” from the “Storm Control (broadcast and multicast)” drop-down list to enable or disable Storm Control (broadcast and multicast) for Chain Protocol setting.

5. Submit: Click “Submit” button when you finished Chain Protocol setting.

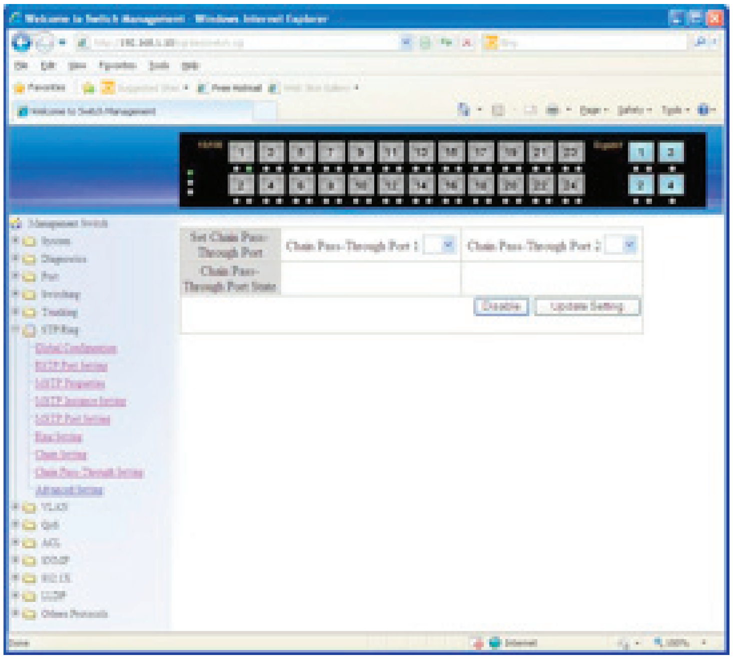

Set Chain Pass-Through Port
Chain Pass-Through Port 1
Chain Pass-Through Port 2
Chain Pass-Through Port State
Disable
Update Setting

Figure 6-46.

Chain Pass-Through Setting

1. Chain pass-through port 1: Choose Chain pass-through port 1 from the “Chain pass-through port 1” drop-down list.

2. Chain pass-through port 2: Click “Choose Chain pass-through port 2 from the “Chain pass-through port 2” drop-down list.

3. Disable: Click on the “Disable” button to disable chain pass-through setting.

4. Update Setting: Click on the “Update Setting” button when you finish chain pass-through setting.

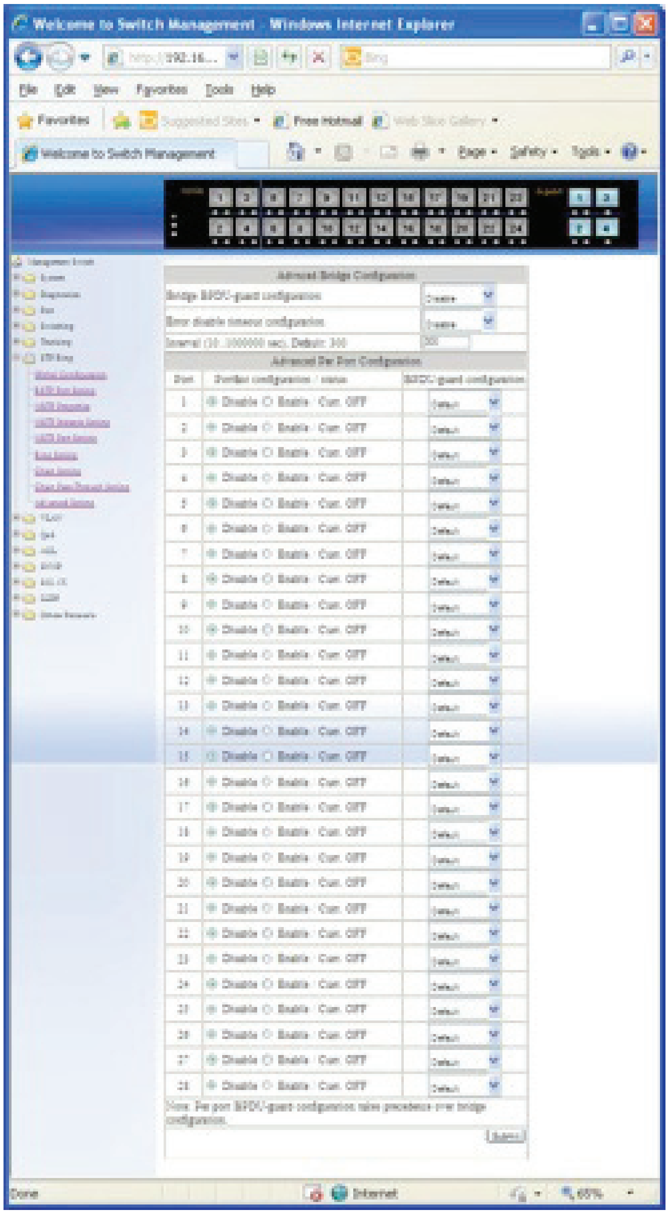


Figure 6-47.

Advanced Setting

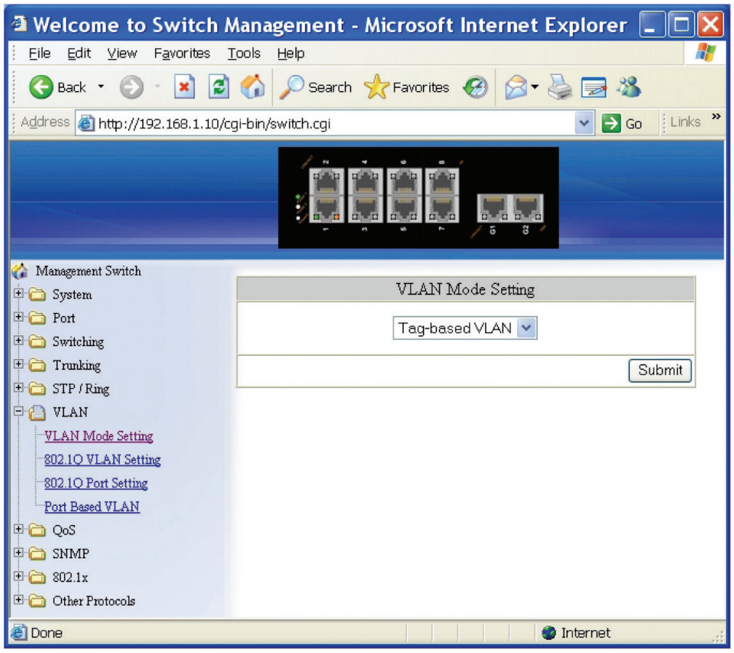
Advanced Bridge Configuration:

1. Bridge bpdu-guard cofiguration: Choose "Enable" or "Disable" from the "Bridge bpdu-guard cofiguration" drop-down list to enable or disable the portfast ports to guard against bpdu received for a bridge. When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have bpdu-guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
2. Error disable timeout cofiguration: Choose "Enable" or "Disable" from the "Error disable timeout cofiguration" drop-down list to enable or disable the timeout mechanism for the port to be enabled back for a bridge.
3. Interval (10..1000000 sec), Default: 300: Click in the text box and type a decimal number as interval time in seconds after which a port will be enabled for a bridge.

Advanced Per Port Configuration:

1. Portfast configuration/status: Click and choose “Disable” or “Enable” to disable or enable a port as an edge-port to enable rapid transition.
2. Bpdu-guard configuration: Choose “Enable,” “Disable,” or “Default” from the “Bpdu-guard configuration” drop-down list to enable, disable, or default the BPDU Guard feature on a port. This command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge level BPDU-Guard configuration takes effect.
3. Submit: Click on the “Submit” button when you finish Advanced Setting.

6.9 VLAN


Welcome to Switch Management - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Submit
Done
Internet

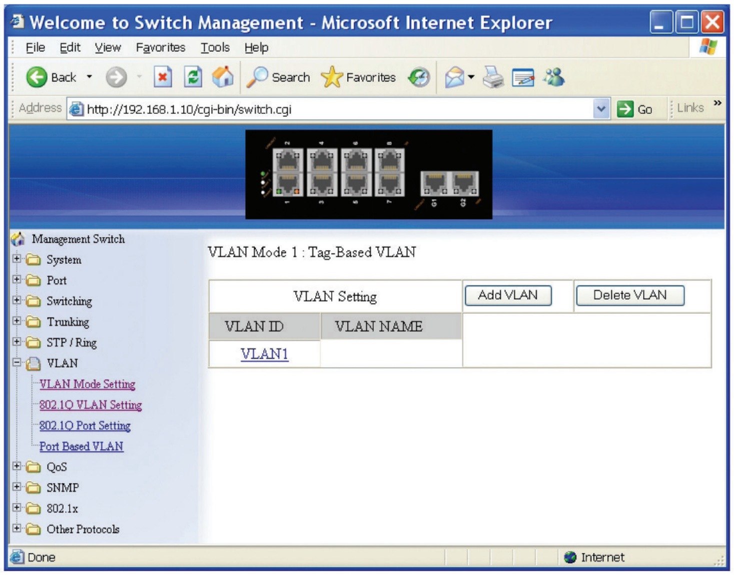
VLAN Mode Setting

Tag-based VLAN

Figure 6-48.

VLAN Mode Setting

1. VLAN Mode Setting: Choose “Tag-based VLAN” or “Port-based VLAN” from the “VLAN Mode Setting” drop-down list.
2. Submit: Click on the “Submit” button when you finish VLAN Mode Setting.

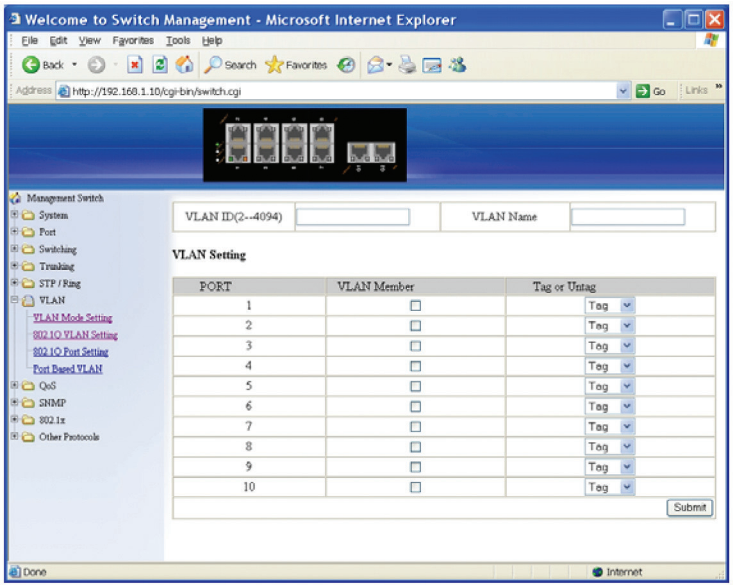

Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Add VLAN
Delete VLAN
Done
Internet

VLAN Mode 1 : Tag-Based VLAN

VLAN Setting

VLAN ID	VLAN NAME
VLAN1	

Figure 6-49.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Submit
Done
Internet

VLAN ID(2--4094)

VLAN Name

VLAN Setting

PORT	VLAN Member	Tag or Untag
1	☐	Tag
2	☐	Tag
3	☐	Tag
4	☐	Tag
5	☐	Tag
6	☐	Tag
7	☐	Tag
8	☐	Tag
9	☐	Tag
10	☐	Tag

Figure 6-50.

802.1Q VLAN Setting

Add VLAN:

1. 802.1Q VLAN Setting: Click “802.1Q VLAN Setting.” The “VLAN Setting” window appears.
2. Add VLAN: Click “Add VLAN” button to create a new VLAN from the “VLAN Setting” window.
3. VLAN ID (2–4094): Click in the “VLAN ID” text box and specify a new VLAN ID number from 2–4094.
4. VLAN Name: Click in the “VLAN Name” text box and type a name for this newly created VLAN.

Add a port to or a delete port from VLAN:

1. VLAN Member: Choose the port to be added to or deleted from the VLAN.

2. Tag or Untag: Click on the “Tag or Untag” drop-down menu to choose “Tag” or “Untag” from the “Tag or Untag” drop-down list for a “Hybrid” port.

3. Submit: Click on the “Submit” button when you finish VLAN setting.

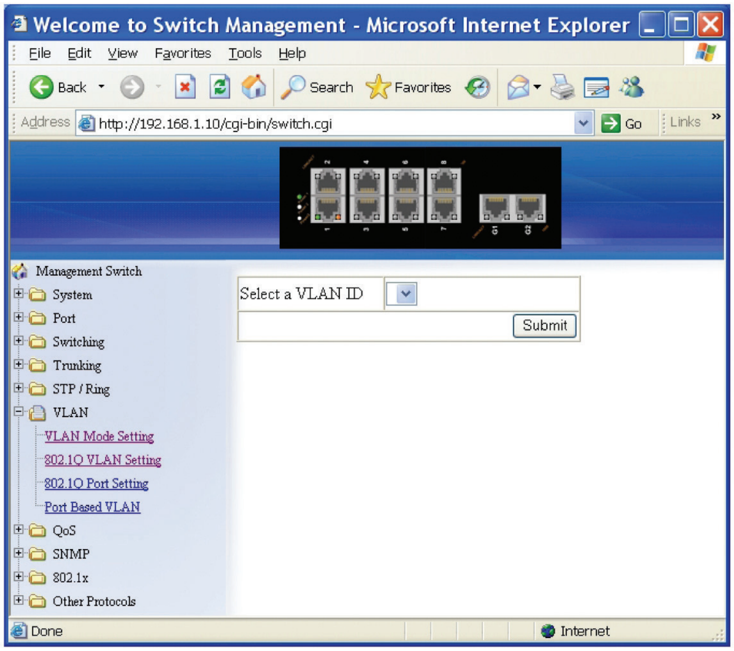

Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Select a VLAN ID
Submit
Done
Internet

Figure 6-51.

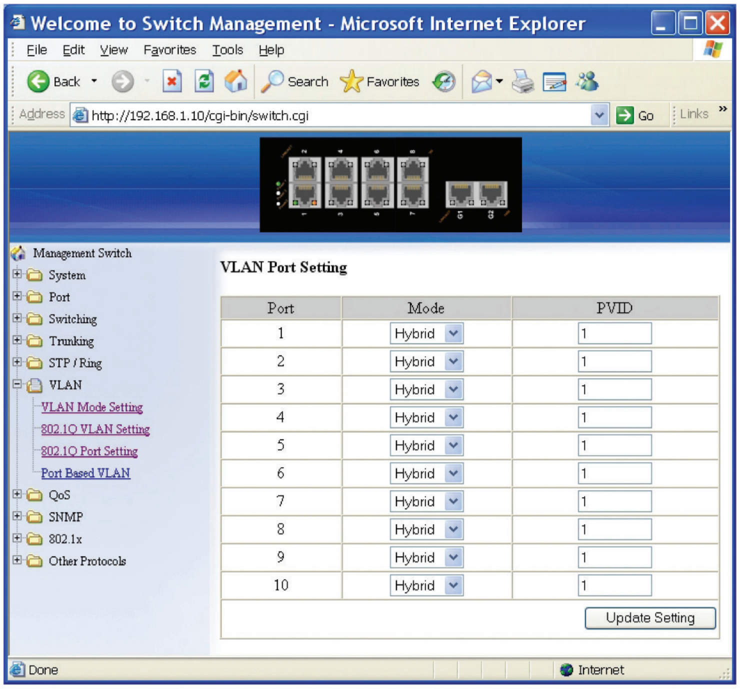
Delete VLAN:

1. 802.1Q VLAN Setting: Click on “802.1Q VLAN Setting.” The “VLAN Setting” window appears.

2. Delete VLAN: Click on the “Delete VLAN” button.

3. Select a VLAN ID: Click “Select a VLAN ID” drop-down menu from “Select a VLAN ID” drop-down list to choose the VLAN to be deleted.

4. Submit: Click on the “Submit” button when you finish VLAN setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Update Setting
Done
Internet

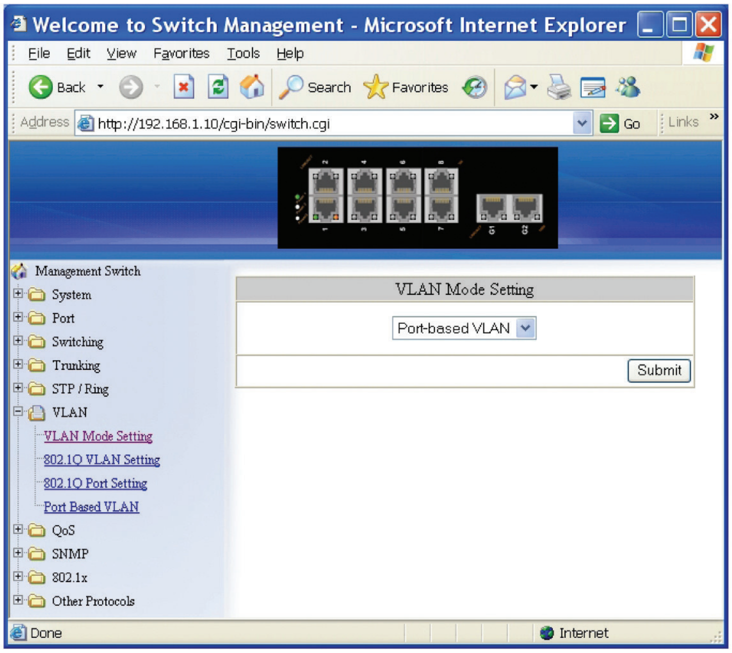
VLAN Port Setting

Port	Mode	PVID
1	Hybrid	1
2	Hybrid	1
3	Hybrid	1
4	Hybrid	1
5	Hybrid	1
6	Hybrid	1
7	Hybrid	1
8	Hybrid	1
9	Hybrid	1
10	Hybrid	1

Figure 6-52.

802.1Q Port Setting

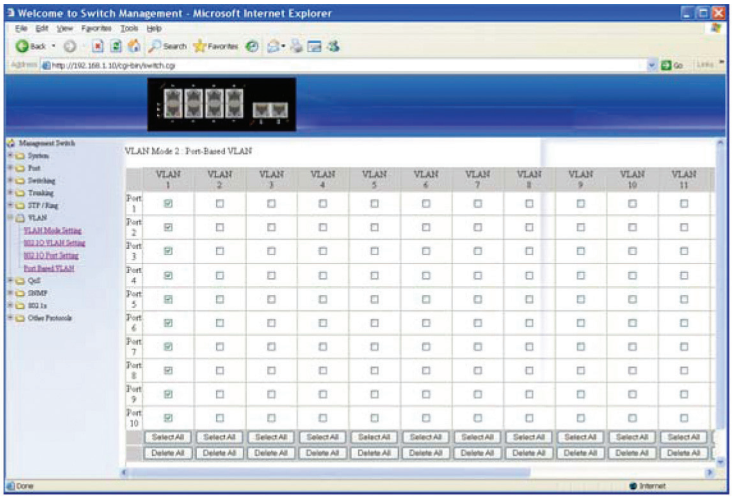
1. VLAN Port Setting: Click on the “802.1Q Port Setting.” The “VLAN Port Setting” window appears.
2. Mode: Click on the “Mode” drop-down menu to choose “Access,” “Trunk,” or “Hybrid” from the “Mode” drop-down list for the port. The port will be a Tag port if you choose “Trunk” Mode for the port. And the port will be a Tag or Untag port if you choose “Hybrid” Mode for the port.
3. PVID: Click in the “PVID” textbox and specify a new PVID number for the port.
4. Priority Level: Click in the “Priority Level” text box and specify a new Priority Level number from 0 ~ 7 for the port. The default Priority Level number is 0.
5. Update Setting: Click on the “Update Setting” button when you finish VLAN Port Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Submit
Done
Internet

VLAN Mode Setting

Port-based VLAN

Figure 6-53.


Welcome to Switch Management - Microsoft Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
SNMP
802.1x
Other Protocols
Done
Internet

VLAN Mode 2 : Port-Based VLAN

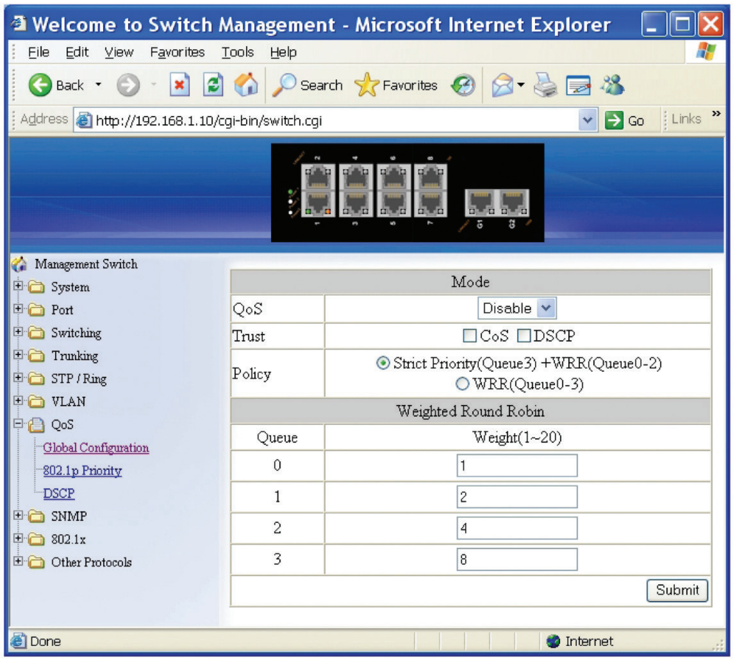
	VLAN 1	VLAN 2	VLAN 3	VLAN 4	VLAN 5	VLAN 6	VLAN 7	VLAN 8	VLAN 9	VLAN 10	VLAN 11
Port 1	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 2	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 3	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 4	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 5	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 6	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 7	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 8	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 9	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Port 10	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	Select All	Select All	Select All	Select All	Select All	Select All	Select All	Select All	Select All	Select All	Select All
	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All

Figure 6-54.

Port Based VLAN

1. VLAN: Choose the port to be added to or deleted from the VLAN.
2. Select All: Click on the "Select All" button to choose all ports to be added to the VLAN.
3. Delete All: Click on the "Delete All" button to choose all ports to be deleted from the VLAN.
4. Submit: Click on the "Submit" button when you finish Port-Based VLAN setting.

6.10 QoS

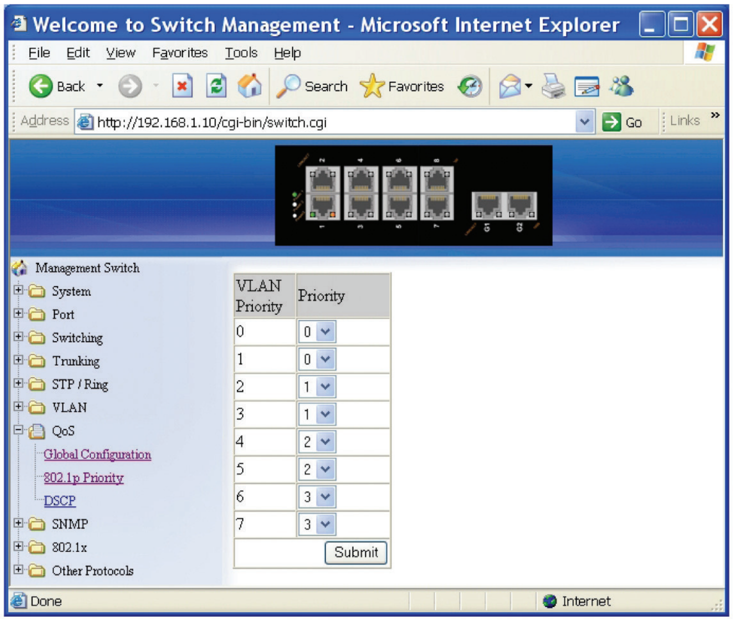

Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
Global Configuration
802.1p Priority
DSCP
SNMP
802.1x
Other Protocols
Done
Internet

Mode	
QoS	Disable
Trust	☐CoS ☐DSCP
Policy	● Strict Priority(Queue3) +WRR(Queue0-2) ○ WRR(Queue0-3)
Weighted Round Robin	
Queue	Weight(1~20)
0	1
1	2
2	4
3	8
	Submit

Figure 6-55.

Global Configuration

1. QoS: From the “QoS” drop-down list, choose “Enable” or “Disable” to enable or disable QoS.
2. Trust: Enable or disable the switch port to trust the CoS (Class of Service) labels of all traffic received on that port. Enable or disable a routed port to trust the DSCP (Differentiated Service Code Point) labels of all traffic received on that port.
3. Policy: Choose “Strict Priority(Queue3) + WRR(Queue0-2)” or “WRR(Queue0-3).” A strict priority queue is always emptied first. The queues that are used in the WRR (Weighted Round Robin) are emptied in a round–robin fashion, and you can configure the weight for each queue.
4. Weighted Round Robin: Click in the “Weight (1–55)” text box and specify a new number from 1–55 for Queue 0–3.
5. Submit: Click on the “Submit” button when you finish Global Configuration.


Welcome to Switch Management - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
Global Configuration
802.1p Priority
DSCP
SNMP
802.1x
Other Protocols
Submit
Done
Internet

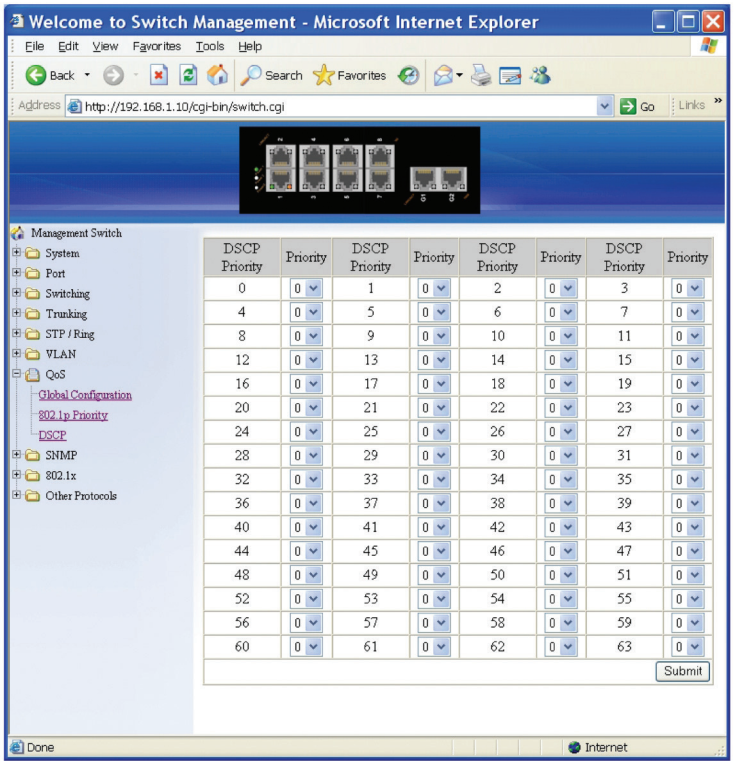
VLAN Priority	Priority
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Figure 6-56.

802.1p Priority

1. Priority: From the "Priority" drop-down list, choose 0–3 for VLAN Priority 0–7.

2. Submit: Click on the "Submit" button when you finish 802.1p priority.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
Global Configuration
802.1p Priority
DSCP
SNMP
802.1x
Other Protocols
Submit
Done
Internet

DSCP Priority	Priority	DSCP Priority	Priority	DSCP Priority	Priority	DSCP Priority	Priority
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	0	9	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0
32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0
60	0	61	0	62	0	63	0

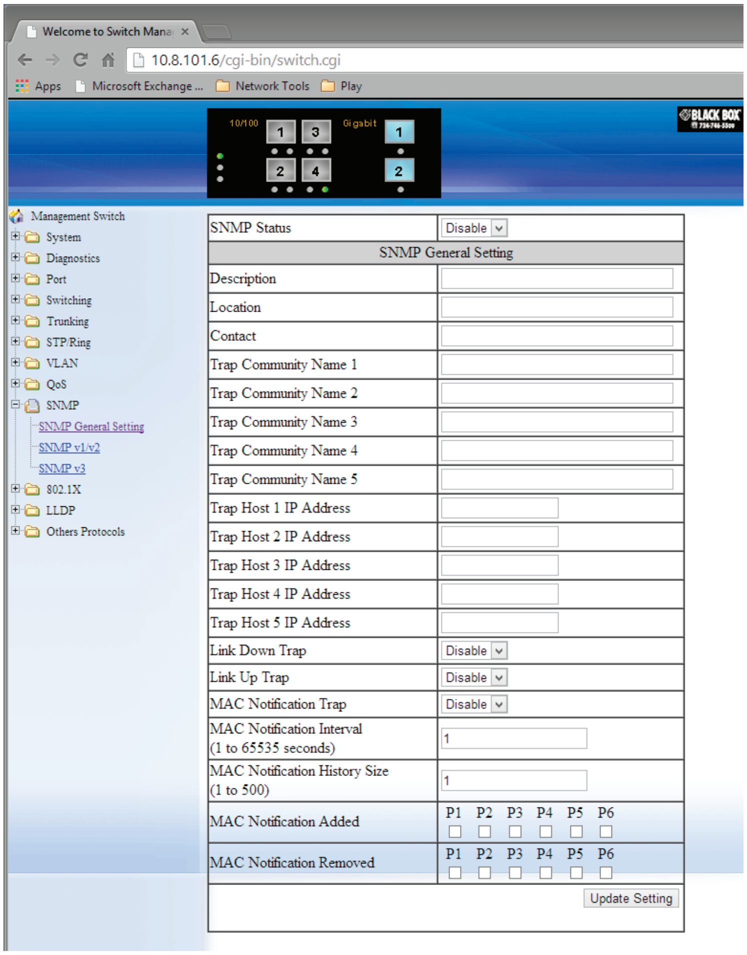
Figure 6-57.

DSCP

1. Priority: From “Priority” drop-down list, choose 0–3 for DSCP Priority 0–63.

2. Submit: Click on the “Submit” button when you finish DSCP.

6.11 SNMP


Welcome to Switch Mana
10.8.101.6/cgi-bin/switch.cgi
Apps
Microsoft Exchange ...
Network Tools
Play
10/100
1
3
2
4
Gigabit
1
2
BLACK BOX
724-746-5500
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
SNMP
SNMP General Setting
SNMP v1/v2
SNMP v3
802.1X
LLDP
Others Protocols
Update Setting

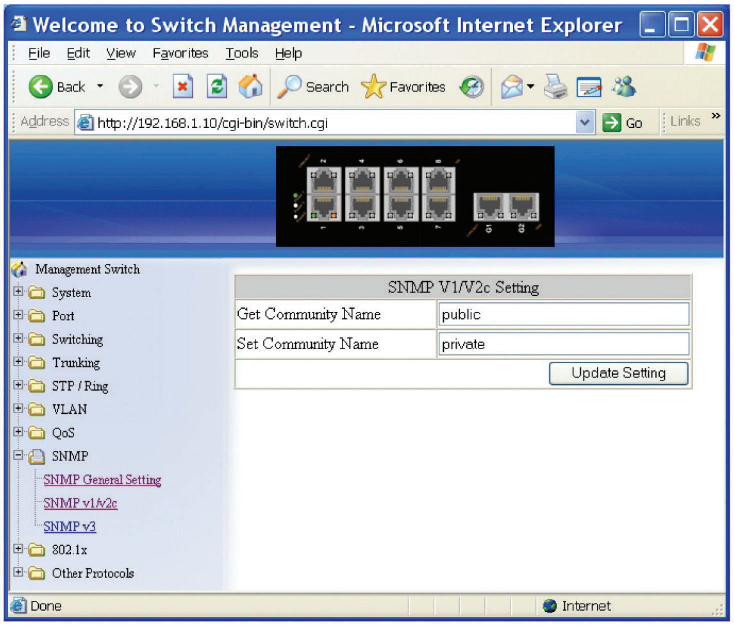
SNMP Status	Disable
SNMP General Setting	
Description	
Location	
Contact	
Trap Community Name 1	
Trap Community Name 2	
Trap Community Name 3	
Trap Community Name 4	
Trap Community Name 5	
Trap Host 1 IP Address	
Trap Host 2 IP Address	
Trap Host 3 IP Address	
Trap Host 4 IP Address	
Trap Host 5 IP Address	
Link Down Trap	Disable
Link Up Trap	Disable
MAC Notification Trap	Disable
MAC Notification Interval (1 to 65535 seconds)	1
MAC Notification History Size (1 to 500)	1
MAC Notification Added	P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6 ☐
MAC Notification Removed	P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6 ☐

Figure 6-58.

SNMP General Setting

1. SNMP Status: From the "SNMP Status" drop-down list, choose "Enable" or "Disable" to enable or disable SNMP.
2. Description: Click in the "Description" text box and specify a new description for SNMP.
3. Location: Click in the "Location" text box and specify a new location for SNMP.
4. Contact: Click in the "Contact" text box and specify a new contact for SNMP.
5. Trap Community Name: Click in the "Trap Community Name" textbox and specify a trap community name.
6. Trap Host IP Address: Click in the "Trap Host IP Address" textbox and specify a trap host IP address.
7. Link Down Trap: From the "Link Down Trap" drop-down list, choose "Enable" or "Disable" to enable or disable link down trap.
8. Link Up Trap: From the "Link Up Trap" drop-down list, choose "Enable" or "Disable" to enable or disable link up trap.
9. MAC Notification Trap: From the "MAC Notification Trap" drop-down list, choose "Disable" or "Enable" to disable or enable the Switch to send MAC Notification Trap to the network management system (NMS).
10. MAC Notification Interval (1 to 65535 seconds): Click the text box and type a decimal number to configure the MAC notification interval in seconds. The range is 1 to 65535 seconds. The switch sends the MAC Notification Trap when this amount of time has elapsed.

11. MAC Notification History Size (1 to 500): Click the text box and type a decimal number to configure the maximum number of entries in the MAC notification history table. The range is 1 to 500.
12. MAC Notification Added: Click and choose the port to enable MAC Notification Trap on an interface port.
13. MAC Notification Removed: Click and choose the port to disable MAC Notification Trap on an interface port.
14. Update Setting: Click on the "Update Setting" button when you finish SNMP General Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
SNMP General Setting
SNMP v1/v2c
SNMP v3
802.1x
Other Protocols
Update Setting
Done
Internet

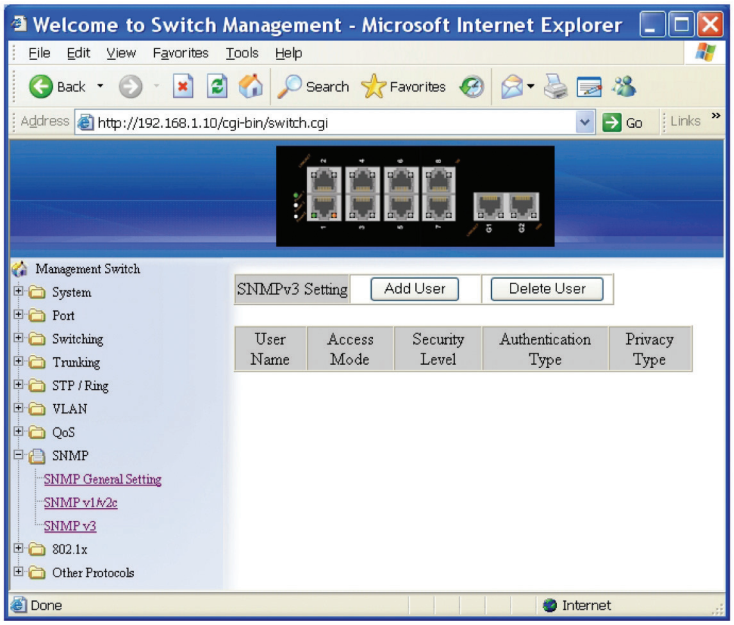
SNMP V1/V2c Setting

Get Community Name	public
Set Community Name	private

FIgure 6-59.

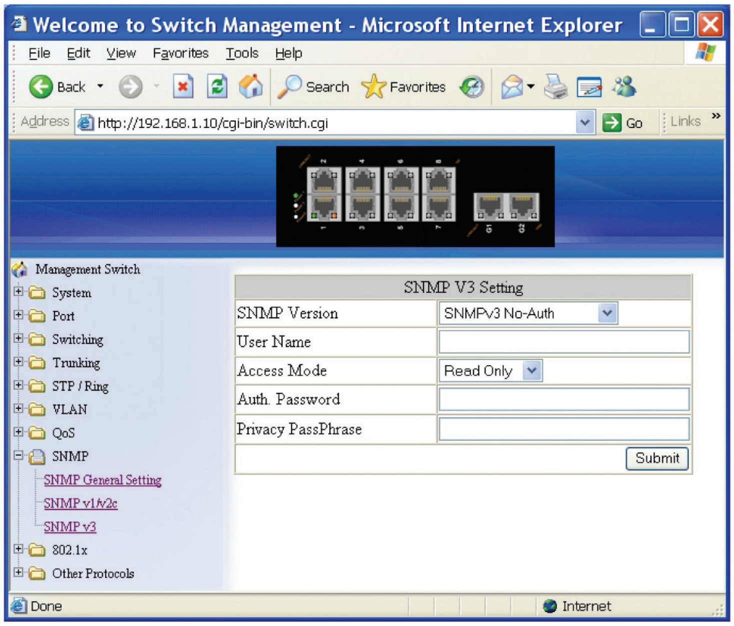
SNMP v1/v2c

1. Get Community Name: Click in the "Get Community Name" textbox and specify a get community name.
2. Set Community Name: Click in the "Set Community Name" textbox and specify a set community name.
3. Update Setting: Click "Update Setting" button when you finished SNMP V1/V2c Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
SNMP General Setting
SNMP v1/v2c
SNMP v3
802.1x
Other Protocols
SNMPv3 Setting
Add User
Delete User
User Name
Access Mode
Security Level
Authentication Type
Privacy Type
Done
Internet

Address: http://192.168.1.10/cgi-bin/switch.cgi

Figure 6-60.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
SNMP General Setting
SNMP v1/v2c
SNMP v3
802.1x
Other Protocols
SNMP V3 Setting
Submit
Done
Internet

Address: http://192.168.1.10/cgi-bin/switch.cgi

SNMP V3 Setting	
SNMP Version	SNMPv3 No-Auth
User Name	
Access Mode	Read Only
Auth. Password	
Privacy PassPhrase	

Figure 6-61.

SNMP v3

Add User:

1. Add User: Click “Add User” button. The “SNMP V3 Setting” window appears.

2. SNMP Version: From the “SNMP Version” drop-down list, choose “SNMPv3 No-Auth,” “SNMPv3 Auth-MD5,” “SNMPv3 Auth-SHA,” “SNMPv3 Priv Auth-MD5,” or “SNMPv3 Priv Auth-SHA.”

- SNMPv3 No-Auth: Add a user using SNMP v3 without authentication.

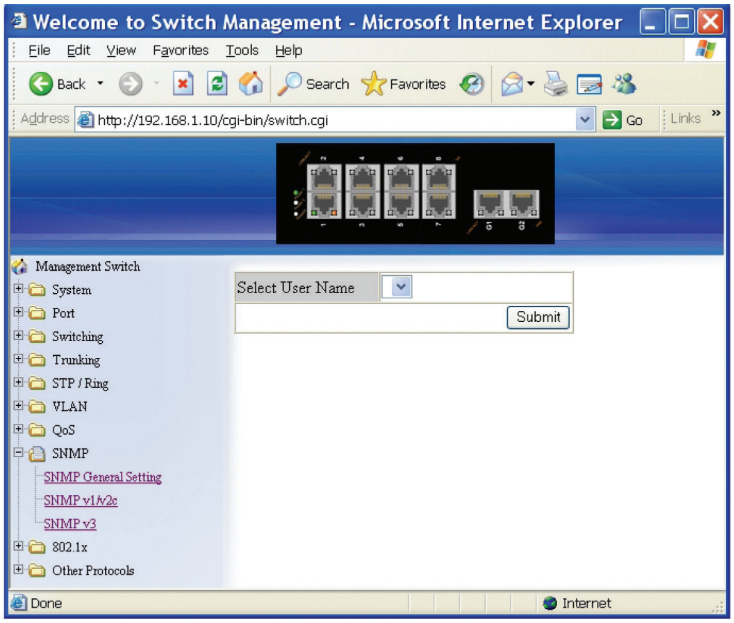
- SNMPv3 Auth-MD5: Add a user using SNMP v3 with authentication. Click in the “Auth. Password” textbox and specify an authentication password.
- SNMPv3 Auth-SHA: Add a user using SNMP v3 with authentication. Click in the “Auth. Password” textbox and specify an authentication password.
- SNMPv3 Priv Auth-MD5: Add a user using SNMP v3 with authentication and privacy. Click in the “Auth. Password” textbox and specify an authentication password. Click in the “Privacy PassPhrase” textbox and specify a privacy pass phrase.
- SNMPv3 Priv Auth-SHA: Add a user using SNMP v3 with authentication and privacy. Click in the “Auth. Password” textbox and specify an authentication password. Click in the “Privacy PassPhrase” textbox and specify a privacy pass phrase.

3. User Name: Click in the “User Name” textbox and specify a user name for a user using SNMP v3.

4. Access Mode: From the “Access Mode” drop-down list, choose “Read Only” or “Read/Write.”

- Read Only: Add a user using SNMP v3 with read-only access mode.
- Read/Write: Add an user using SNMP v3 with read-write access mode.

5. Submit: Click on the “Submit” button when you finish SNMP V3 Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
SNMP General Setting
SNMP v1/v2c
SNMP v3
802.1x
Other Protocols
Done
Internet

http://192.168.1.10/cgi-bin/switch.cgi

Select User Name

Submit

FIgure 6-62.

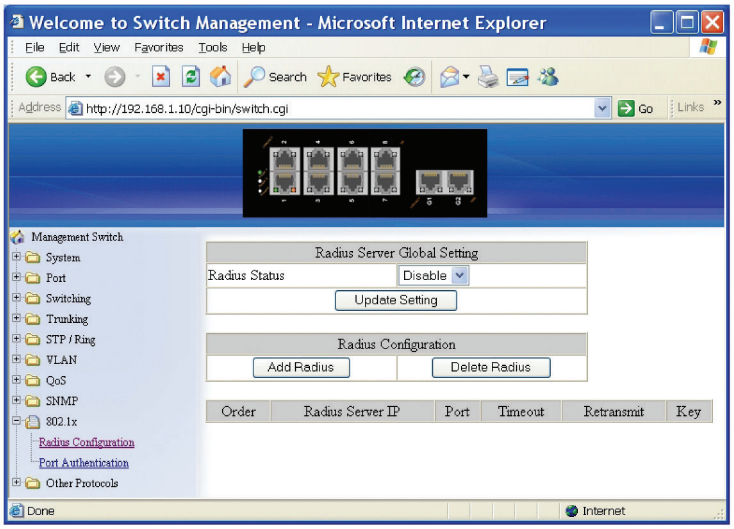
Delete User:

1. Delete User: Click on the “Delete User” button. The “Select User Name” window appears.

2. Select User Name: From the “Select User Name” drop-down list, choose the user to be deleted from using SNMP v3.

3. Submit: Click on the “Submit” button when you finish user deletion.

6.12 802.1x


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Radius Configuration
Port Authentication
Other Protocols
Done
Internet

Radius Server Global Setting	
Radius Status	Disable

Update Setting

Radius Configuration

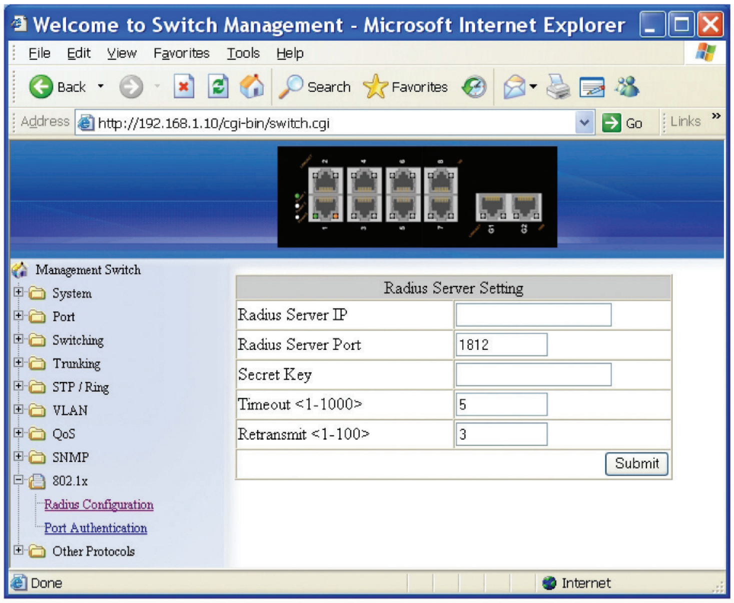
Add Radius Delete Radius

Order	Radius Server IP	Port	Timeout	Retransmit	Key

Figure 6-63.

Radius Configuration

1. Radius Status: From the "Radius Status" drop-down list, choose "Enable" or "Disable" to globally enable or disable authentication.
2. Update Setting: Click on the "Update Setting" button when you finish Radius Status Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Radius Configuration
Port Authentication
Other Protocols
Done
Internet

Radius Server Setting	
Radius Server IP	
Radius Server Port	1812
Secret Key	
Timeout <1-1000>	5
Retransmit <1-100>	3

Submit

Figure 6-64.

Add Radius:

1. Add Radius: Click on the "Add Radius" button. The "Radius Server Setting" window appears.
2. Radius Server IP: Click in the "Radius Server IP" text box and specify the IP address of the remote radius server host.

3. Radius Server Port: Click in the "Radius Server Port" text box and specify the UDP destination port for authentication requests. The host is not used for authentication if set to 0.

4. Secret Key: Click in the "Secret Key" text box and specify the authentication and encryption key for all radius communications between the Switch and radius server. This key must match the encryption used on the radius daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If spaces are used in the key, do not enclose the key in quotaion marks unless the quotation marks themselves are part of the key.

5. Timeout <1-1000>: Click in the "Timeout" text box and specify the time interval (in seconds) that the Switch waits for the radius server to reply before retransmitting. Enter a value in the range 1 to 1000.

6. Retransmit <1-100>: Click in the "Retransmit" text box and specify the number of times a radius request is resent to a server if that server is not responding or responding slowly. Enter a value in the range 1 to 100.

7. Submit: Click on the "Submit" button when you finish Radius Server Setting.

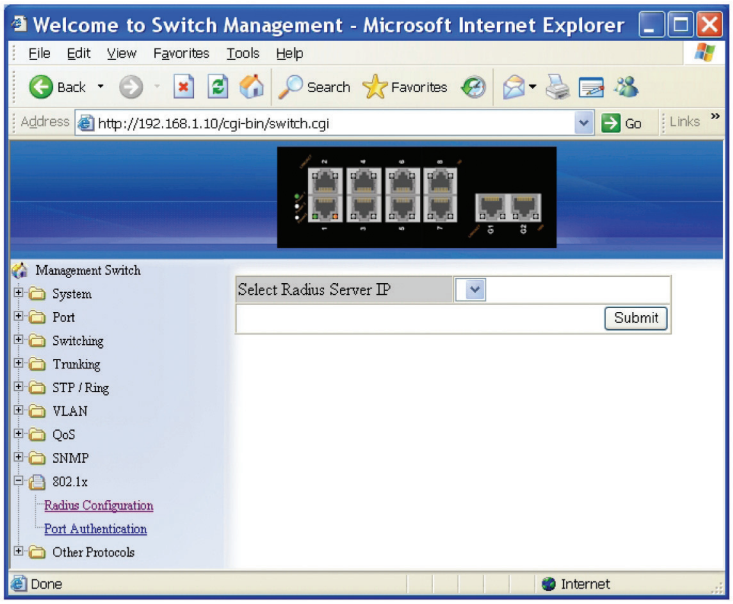

Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Radius Configuration
Port Authentication
Other Protocols
Select Radius Server IP
Submit
Done
Internet

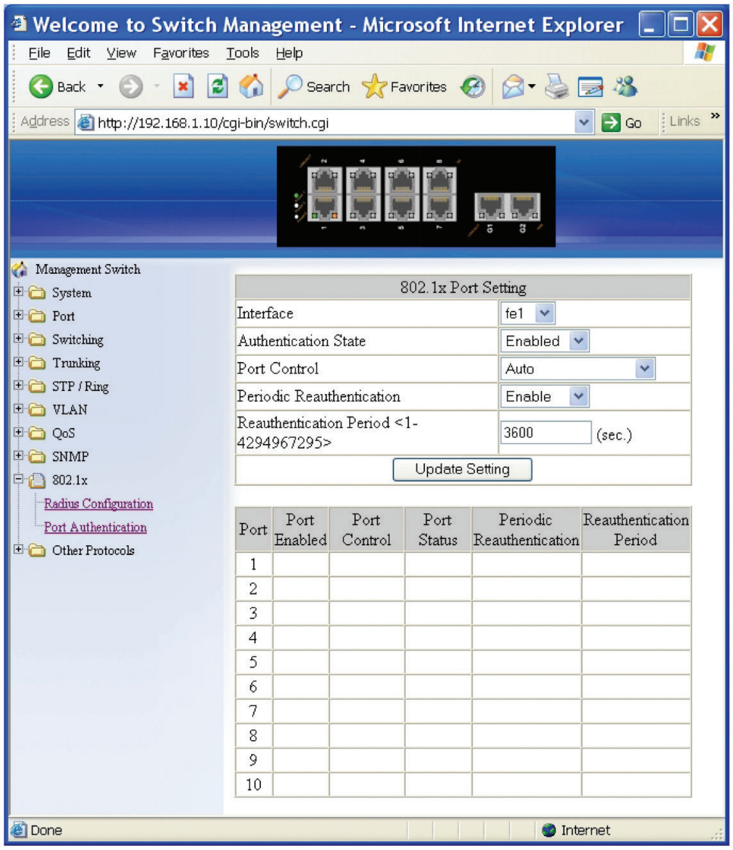
Figure 6-65.

Delete Radius:

1. Delete Radius: Click on the "Delete Radius" button. The "Select Radius Server IP" window appears.

2. Select Radius Server IP: From the "Select Radius Server IP" drop-down list, choose the IP address of the remote radius server host to be deleted.

3. Submit: Click on the "Submit" button when you finish radius server deletion.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Radius Configuration
Port Authentication
Other Protocols
Update Setting
Done
Internet

802.1x Port Setting	
Interface	fe1
Authentication State	Enabled
Port Control	Auto
Periodic Reauthentication	Enable
Reauthentication Period <1-4294967295>	3600 (sec.)

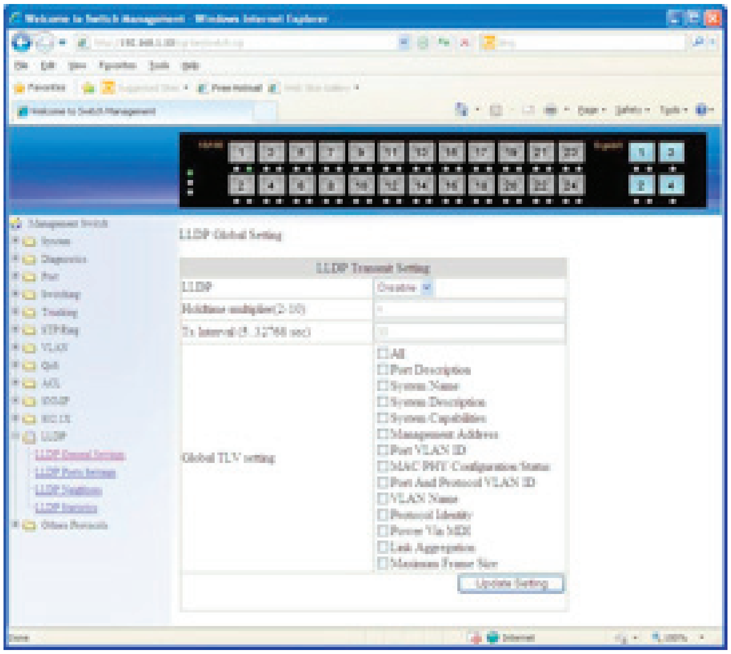
Port	Port Enabled	Port Control	Port Status	Periodic Reauthentication	Reauthentication Period
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Figure 6-66.

Port Authentication

1. Interface: From the “Interface” drop-down list, choose the port to set port-based authentication.
2. Authentication State: From the “Authentication State” drop-down list, choose “Enable” or “Disable” to enable or disable authentication state.
3. Port Control: From the “Port Control” drop-down list, choose “Auto,” “Force Authorized,” or “Force Unauthorized” to force a port state. “Auto” specifies to enable authentication on port. “Force Authorized” specifies to force a port to always be in an authorized state. “Force Unauthorized” specifies to force a port to always be in an unauthorized state.
4. Periodic Reauthentication: From the “Periodic Reauthentication” drop-down list, choose “Enable” or “Disable” to enable or disable periodic reauthentication.
5. Reauthentication Period <1-4294967295>: Click in the “Reauthentication Period” textbox and specify the seconds between reauthorization attempts. The default time is 3600 seconds.
6. Update Setting: Click on the “Update Setting” button when you finish port-based authentication setting.

6.13 LLDP


Welcome to Switch Management
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
IGMP
802.1X
LLDP
LLDP General Settings
LLDP Ports Settings
LLDP Neighbors
LLDP Statistics
Others Protocols
Update Setting

LLDP Global Setting

LLDP Transmit Setting	
LLDP	Disable
Holdtime multiplier(2-10)	4
Tx Interval(5..32768 sec)	
Global TLV setting	☐ All ☐ Port Description ☐ System Name ☐ System Description ☐ System Capabilities ☐ Management Address ☐ Port VLAN ID ☐ MAC PHY Configuration Status ☐ Port And Protocol VLAN ID ☐ VLAN Name ☐ Protocol Identity ☐ Power Via MDI ☐ Link Aggregation ☐ Maximum Frame Size

Figure 6-67.

LLDP General Settings

1. LLDP: From the “LLDP” drop-down list, choose “Enable” or “Disable” to enable or disable Link Layer Discovery Protocol (LLDP) globally.
2. Holdtime multiplier (2-10): Click in the “Holdtime multiplier” textbox and set the Link Layer Discovery Protocol (LLDP) holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) that the switch advertises to the neighbors. Enter a Holdtime multiplier value in the range from 2 to 10. Default is 4.
3. Tx Interval (5-32768 seconds): Click in the “Tx Interval” text box and set the transmit interval. This is the interval between regular transmissions of Link Layer Discovery Protocol (LLDP) advertisements. Enter a Tx Interval value in the range from 5 to 32768. Default is 30 seconds.
4. Global TLV setting: Click and choose Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.
5. Update Setting: Click on the “Update Setting” button when you finish LLDP General Settings.

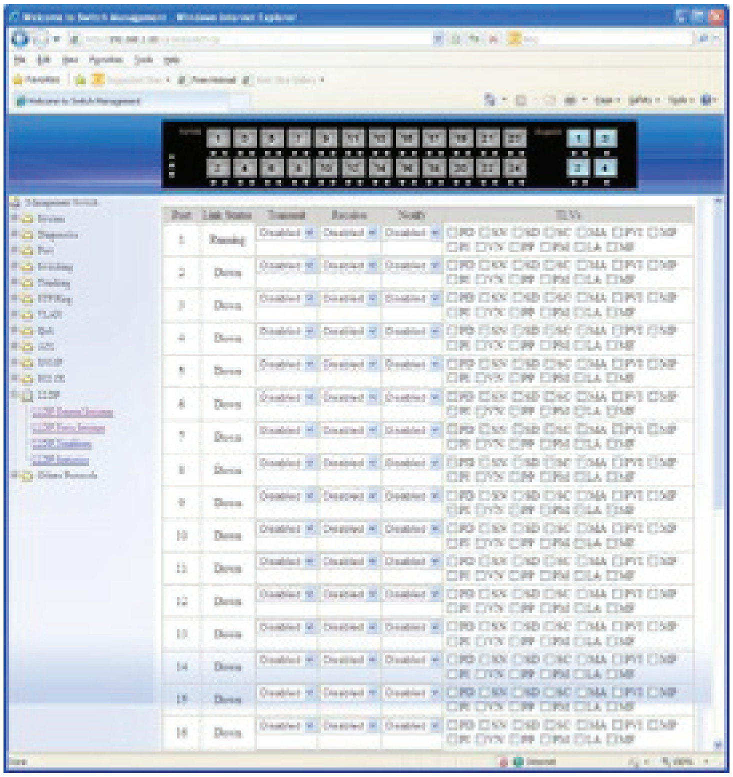
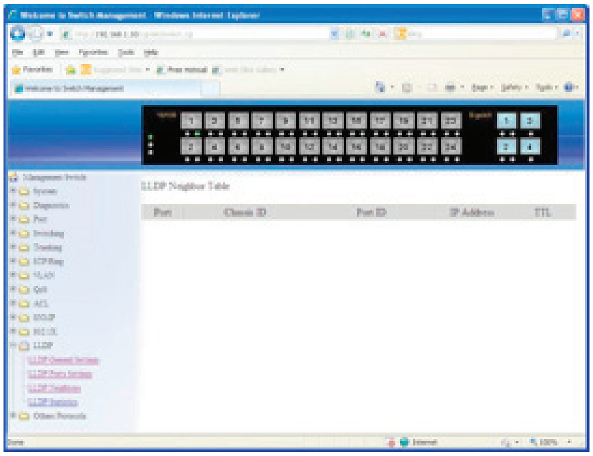


Figure 6-68.

LLDP Ports Settings

1. Transmit: From the “Transmit” drop-down list, choose “Disable” or “Enable” to disallow or allow sending Link Layer Discovery Protocol (LLDP) packets on the interface.
2. Receive: From the “Receive” drop-down list, choose “Disable” or “Enable” to disallow or allow receiving Link Layer Discovery Protocol (LLDP) packets on the interface.
3. Notify: From the “Notify” drop-down list, choose “Disable” or “Enable” to disable or enable Link Layer Discovery Protocol (LLDP) notification on the interface.
4. TLVs: Click and choose Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.
5. Submit: Click on the “Submit” button when you finish LLDP Ports Settings.


Welcome to Switch Management - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
IGMP
802.1X
LLDP
LLDP General Settings
LLDP Ports Settings
LLDP Neighbors
LLDP Statistics
Other Protocols
Done
Internet
100%

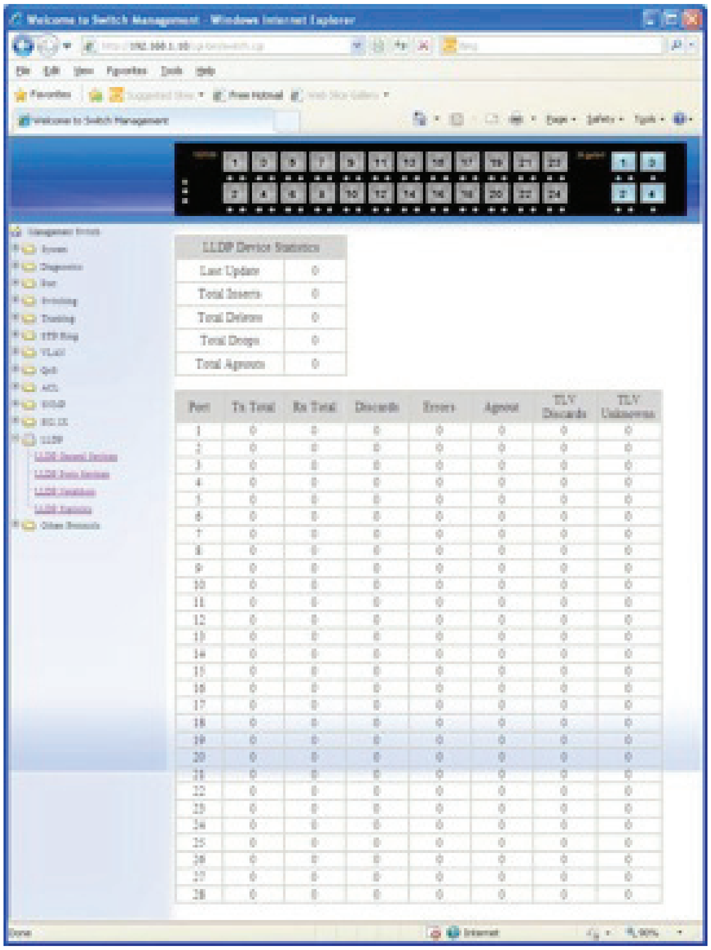
LLDP Neighbor Table

Port	Chassis ID	Port ID	IP Address	TTL

Figure 6-69.

LLDP Neighbors

Click LLDP Neighbors to show Link Layer Discovery Protocol (LLDP) neighbors information.


Welcome to Switch Management - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
IGMP
802.1X
LLDP
LLDP General Settings
LLDP Ports Settings
LLDP Neighbors
LLDP Statistics
Other Protocols
Done
Internet
90%

LLDP Device Statistics	
Last Update	0
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

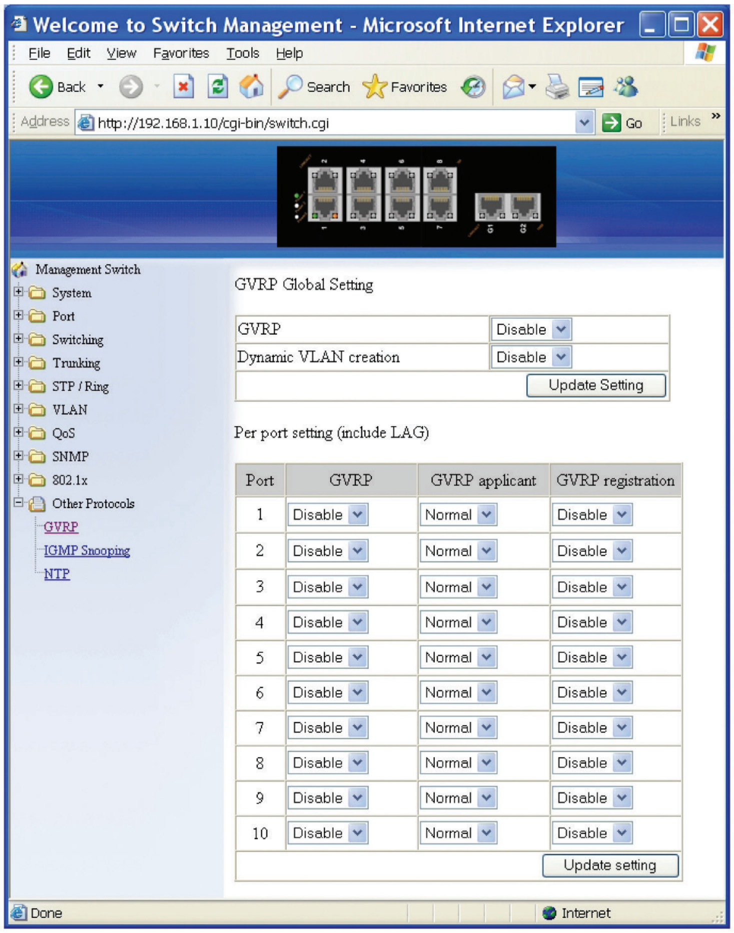
Port	Tx Total	Rx Total	Discards	Errors	Ageout	TLV Discards	TLV Unknowns
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0

Figure 6-70.

LLDP Statistics

Click LLDP Statistics to show Link Layer Discovery Protocol (LLDP) statistics.

6.14 Other Protocols


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
GVRP
IGMP Snooping
NTP
Update Setting
Update setting
Done
Internet

GVRP Global Setting

GVRP	Disable
Dynamic VLAN creation	Disable

Per port setting (include LAG)

Port	GVRP	GVRP applicant	GVRP registration
1	Disable	Normal	Disable
2	Disable	Normal	Disable
3	Disable	Normal	Disable
4	Disable	Normal	Disable
5	Disable	Normal	Disable
6	Disable	Normal	Disable
7	Disable	Normal	Disable
8	Disable	Normal	Disable
9	Disable	Normal	Disable
10	Disable	Normal	Disable

Figure 6-71.

GVRP

GVRP Global Setting:

1. GVRP: From the“GVRP” drop-down list, choose “Enable” or “Disable” to enable or disable GVRP (GARP VLAN Registration Protocol).

2. Dynamic VLAN Creation: From the “Dynamic VLAN Creation” drop-down list, choose “Enable” or “Disable” to enable or disable Dynamic VLAN Creation. GARP (Generic Attribute Registration Protocol) provides IEEE802.1Q compliant VLAN pruning and dynamic VLAN creation on IEEE802.1Q trunk ports.

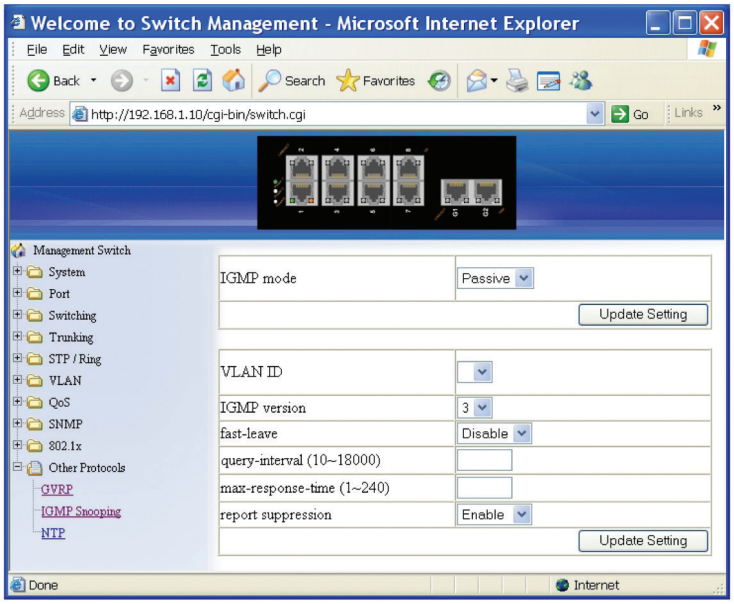
3. Update Setting: Click on the “Update Setting” button when you finish GVRP Global Setting.

Per Port Setting (include LAG):

1. GVRP: From the “GVRP” drop-down list, choose “Enable” or “Disable” to enable or disable GVRP for the port.

2. GVRP Applicant: From the “GVRP Applicant” drop-down list, choose “Active” or “Normal” to the port. Ports in the GVRP active applicant state send GVRP VLAN declarations when they are in the STP (Spanning Tree Protocol) blocking state, which prevents the STP bridge protocol data units (BPDUs) from being pruned from the other port. Ports in the GVRP normal applicant state do not declare GVRP VLANs when in the STP blocking state.

3. GVRP Registration: From the "GVRP Registration" drop-down list, choose "Enable" or "Disable" to enable or disable GVRP Registration to the port. Configuring an IEEE802.1Q trunk port in registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port.
4. Update Setting: Click on the "Update Setting" button when you finish Per Port Setting.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.1.10/cgi-bin/switch.cgi
Go
Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
GVRP
IGMP Snooping
NTP
Update Setting
Update Setting
Done
Internet

IGMP mode	Passive
VLAN ID	
IGMP version	3
fast-leave	Disable
query-interval (10~18000)	
max-response-time (1~240)	
report suppression	Enable

Figure 6-72.

IGMP Snooping

IGMP Snooping:

1. Click on "IGMP Snooping" to change to IGMP Snooping windows.
2. IGMP Mode: From the "IGMP Mode" drop-down list, choose "Disable," "Passive," or "querier" for the switch.
   Disable: Disable IGMP on the switch. Passive: The switch with only multicast-data-forwarding capability.
   Querier: The switch acts as the querier for the network. There is only one querier on a network at any time.
3. Update Setting: Click on the "Update Setting" button when you finished IGMP Mode settings.
4. VLAN ID: From the "VLAN ID" drop-down list, choose the VLAN under configuration for the switch.
5. IGMP Version: From the "IGMP Version" drop-down list, choose "1," "2," or "3" for the switch.
6. Fast Leave: From the "Fast Leave" drop-down list, choose "Enable" or "Disable" for the switch. Enabling this function will allow members of a multicast group to leave the group immediately when an IGMP Leave Report Packet is received by the Switch.

IGMP Querier:

1. Query Interval (1–18000): Click in the "Query Interval" textbox and specify a new number from 1–18000. The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 18000 seconds are allowed. Default = 125.

2. Max Response Time (1–240): Click in the "Max Response Time" textbox and specify a new number from 1–240. This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 240 (seconds). Default = 10.

IGMP Passive Snooping:

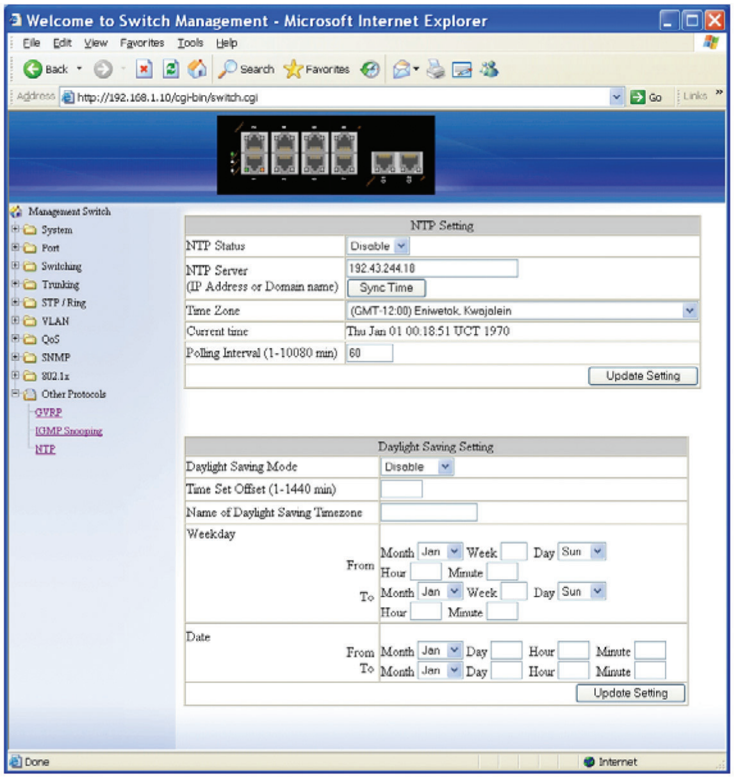
1. Report Suppression: From the "Report Suppression" drop-down list, choose "Enable" or "Disable" for the switch. Use this command to enable report suppression for IGMP version 1 and version 2. Report suppression does not apply to IGMP version 3, and is turned off by default for IGMP version 1 and IGMP version 2 reports. The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled, the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.
2. Update Setting: Click on the "Update Setting" button when you finish IGMP Snooping.

Force Forwarding Port/Passive Mode Forwarding Port:

1. Port: Choose the port to set the port as force forwarding port / passive mode forwarding port. The Switch will forward unknown multicast packets to force forwarding port / passive mode forwarding port before receiving IGMP query.
2. PassiveForwardMode/ForceForwardMode: Click and choose Passive Forward Mode or Force Forward Mode.
3. Update Setting: Click on the "Update Setting" button when you finish Force Forwarding Port or Passive Mode Forwarding Port setting.

Multicast Current Table:

1. Click on "Multicast Current Table" to change to Current Multicast Groups windows.
2. Refresh: Click on the "Refresh" button to refresh Current Multicast Groups information.


Welcome to Switch Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.10/cgi-bin/switch.cgi
Go Links
Management Switch
System
Port
Switching
Trunking
STP / Ring
VLAN
QoS
SNMP
802.1x
Other Protocols
GVRP
IGMP Snooping
NTP
Sync Time
Update Setting
Update Setting
Done
Internet

NTP Setting

NTP Status	Disable
NTP Server (IP Address or Domain name)	192.43.244.18
Time Zone	(GMT-12:00) Eniwetok, Kwajalein
Current time	Thu Jan 01 00:18:51 UCT 1970
Polling Interval (1-10080 min)	60

Daylight Saving Setting

Daylight Saving Mode	Disable
Time Set Offset (1-1440 min)	
Name of Daylight Saving Timezone	
Weekday	From Month Jan Week Day Sun Hour Minute To Month Jan Week Day Sun Hour Minute
Date	From Month Jan Day Hour Minute To Month Jan Day Hour Minute

Figure 6-73.

NTP

Adjust RTC Time:

1. Click in the text box and specify the Year, Month, Day, Hour, Minute, and Second.
2. Update Setting: Click on the “Update Setting” button when you finish Adjust RTC Time.

NTP Setting:

1. NTP Status: From the “NTP Status” drop-down list, choose “Enable” or “Disable” to enable or disable NTP for the Switch.
2. NTP Server (IP Address or Domain name): Click in the “NTP Server” text box and specify the IP address or Domain name of the NTP server.
3. Sync Time: Click on the “Sync Time” button to synchronize time with NTP server.
4. Time Zone: From the “Time Zone” drop-down list, set the time zone.
5. Polling Interval (1–10080 min): Click in the “Polling Interval” textbox and specify the polling interval.
6. Update Setting: Click on the “Update Setting” button when you finish NTP Setting.

Daylight Saving Setting:

1. Daylight Saving Mode: From the "Daylight Saving Mode" drop-down list, choose "Disable," "Weekday," or "Date" to choose disable, weekday, or date daylight saving for the Switch.
2. Time Set Offset (1-1440 min): Click in the "Time Set Offset" textbox and specify the offset time of daylight saving. For example, enter 60 for one hour offset.
3. Name of Daylight Saving Tmiezone: Click in the "Name of Daylight Saving Tmiezone" textbox and specify the name of daylight saving timezone. This can be any given name in 14-character alpha-numericals. Enter the name of Daylight-Saving time zone using the following example:

   EDT - East Daylight Saving Time Zone.

   CDT - Central Daylight-Saving Time Zone.

   MDT - Mountain Daylight-Saving Time Zone.

   PDT - Pacific Daylight-Saving Time Zone.

   ADT - Alaska Daylight-Saving Time Zone.
4. Weekday: Click in the textboxes and specify the daylight saving period.

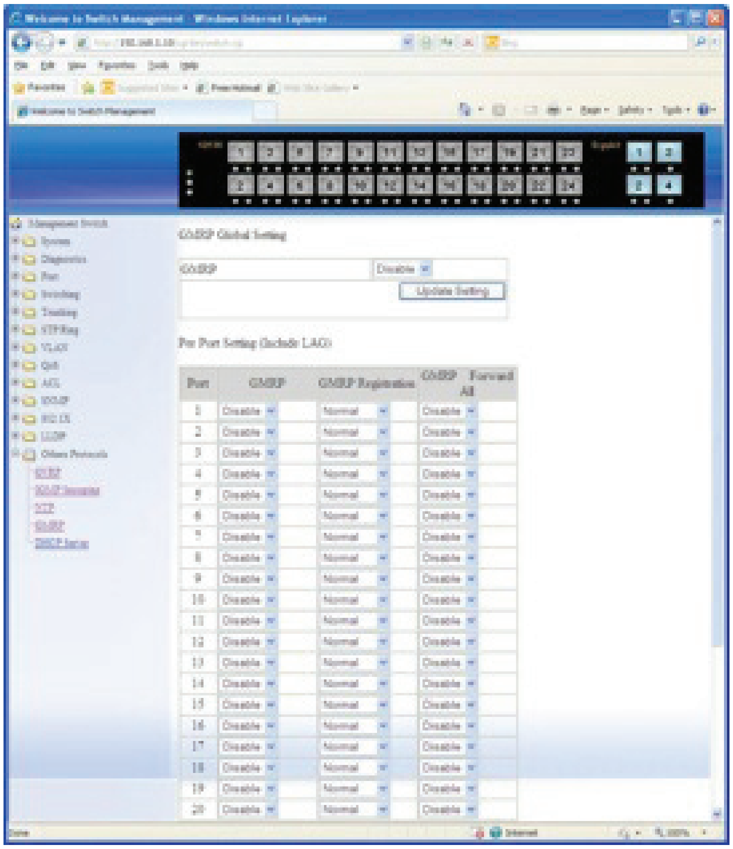
- Month: From the "Month" drop-down list, choose from January to December.
- Week: <1–5> Specifies starting/ending week of daylight savings time.
- Day: From the "Day" drop-down list, choose from Sunday to Saturday.
- Hour: <0–23> Specifies from 0 to 23.
- Minute: <0–59> Specifies from 0 to 59.

5. Date: Click in the textboxes and specify the daylight saving period.

- Month: From the "Month" drop-down list, choose from January to December.
- Day: <1–31> Specifies from 1 to 31.
- Hour: <0–23> Specifies from 0 to 23.
- Minute: <0–59> Specifies from 0 to 59.

6. Update Setting: Click "Update Setting" button when you finish Daylight Saving Setting.

NOTE: The "Week," "Hour," "Minute," and "Day" fields do not accept alphabetic characters (such as Jan, Feb, sun, mon). They only accept two-digit numbers (0 throught 9).


GMRP Global Setting

GMRP: Disable

Update Setting

Per Port Setting (Include LAG)

Port	GMRP	GMRP Registration	GMRP Forward All
1	Disable	Normal	Disable
2	Disable	Normal	Disable
3	Disable	Normal	Disable
4	Disable	Normal	Disable
5	Disable	Normal	Disable
6	Disable	Normal	Disable
7	Disable	Normal	Disable
8	Disable	Normal	Disable
9	Disable	Normal	Disable
10	Disable	Normal	Disable
11	Disable	Normal	Disable
12	Disable	Normal	Disable
13	Disable	Normal	Disable
14	Disable	Normal	Disable
15	Disable	Normal	Disable
16	Disable	Normal	Disable
17	Disable	Normal	Disable
18	Disable	Normal	Disable
19	Disable	Normal	Disable
20	Disable	Normal	Disable

Figure 6-74.

GMRP

GMRP Global Setting:

1. GMRP: From the "GMRP" drop-down list, choose "Enable" or "Disable" to enable or disable GMRP.
2. Update Setting: Click on the "Update Setting" button when you finish GMRP Global Setting.

Per Port Setting (Include LAG):

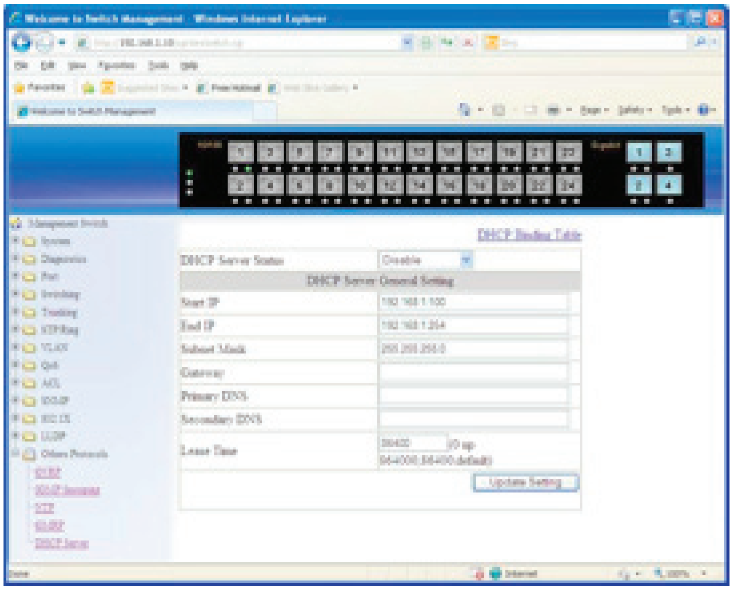
1. GMRP: From the "GMRP" drop-down list, choose "Enable" or "Disable" to enable or disable GMRP for the port.
2. GMRP Registration: From the "GMRP Registration" drop-down list, choose "Normal," "Fixed," or "Forbidden" to specify GMRP Registration to the port.

Normal specifies dynamic GMRP multicast registration and deregistration on the port.

Fixed specifies the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.

Forbidden specifies that all GMRP multicasts are deregistered, and prevents any further GMRP multicast registration on the port.

3. GMRP Forward All: From the "GMRP Forward All" drop-down list, choose "Enable" or "Disable" to enable or disable GMRP forwarding to the port.
4. Update Setting: Click on the "Update Setting" button when you finish Per Port Setting.



DHCP Server Status: Disable

DHCP Server General Setting

Start IP: 192.168.1.100

End IP: 192.168.1.254

Subnet Mask: 255.255.255.0

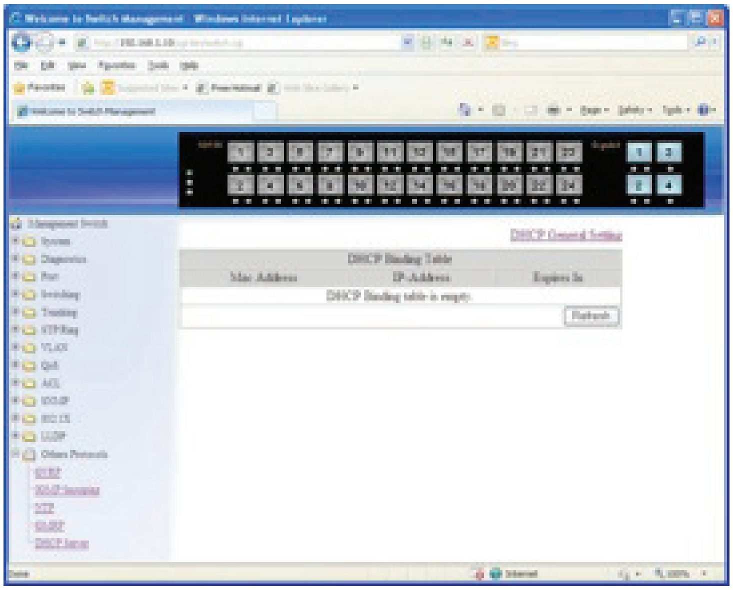
Gateway:

Primary DNS:

Secondary DNS:

Lease Time: 86400 (0 up (864000,86400 default)

Figure 6-75.



DHCP Binding Table		
Mac Address	IP-Address	Expires In
DHCP Binding table is empty.		

Figure 6-76.

DHCP Server

1. DHCP Binding Table: Click on "DHCP Binding Table" to show DHCP Binding Table. Click on the "Refresh" button to refresh DHCP Binding Table. Click on "DHCP General Setting" to back to DHCP General Setting.
2. DHCP Server Status: From the "DHCP Server Status" drop-down list, choose "Disable," "Default VLAN 1," or other VLAN.
3. Start IP: Click in the "Start IP" textbox and specify the default Start IP for the DHCP Server.
4. End IP: Click in the "End IP" textbox and specify the default End IP for the DHCP Server.
5. Subnet Mask: Click in the "Subnet Mask" text box and specify the default subnet mask for the DHCP Server.
6. Gateway: Click in the "Gateway" text box and specify the default gateway for the DHCP Server.

7. Primary DNS: Click in the “Primary DNS” text box and specify the default primary DNS for the DHCP Server.

8. Secondary DNS: Click in the “Secondary DNS” text box and specify the default secondary DNS for the DHCP Server.

9. Lease Time: Click in the “Lease Time” text box and specify the default lease time for the DHCP Server.

10. Update Setting: Click on the “Update Setting” button when you finish DHCP Server General Setting.

7. Command-LIne Management

The switch provides a command-line console interface for configuration purposes. The switch can be configured either locally through its RS-232 port or remotely via a Telnet session. For the latter, you must specify an IP address for the switch first.

This chapter describes how to configure the switch using its console by Command Line.

7.1 Administration Console

Connect the DB9 straight cable to the RS-232 serial port of the device to the RS-232 serial port of the terminal or computer running the terminal emulation application.

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

When using the management method, configure the terminal-emulation program to use the following parameters (you can change these settings after login):

Default parameters:

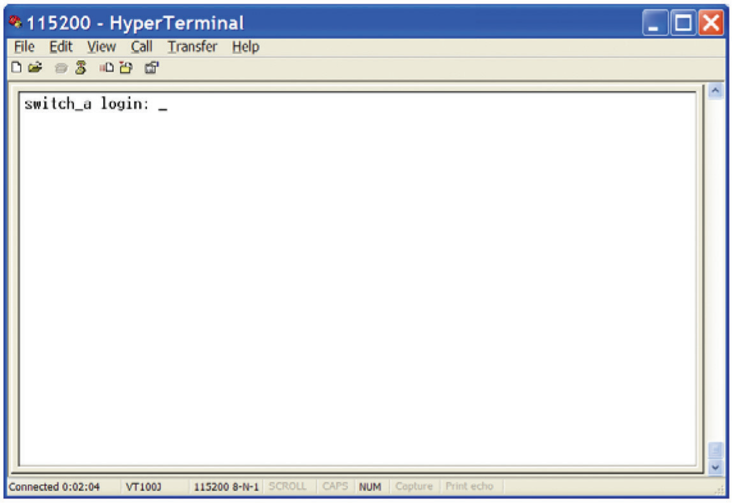
115,200 bps

8 data bits

No parity

1 stop bit

7.1.1 Exec Mode (View Mode)



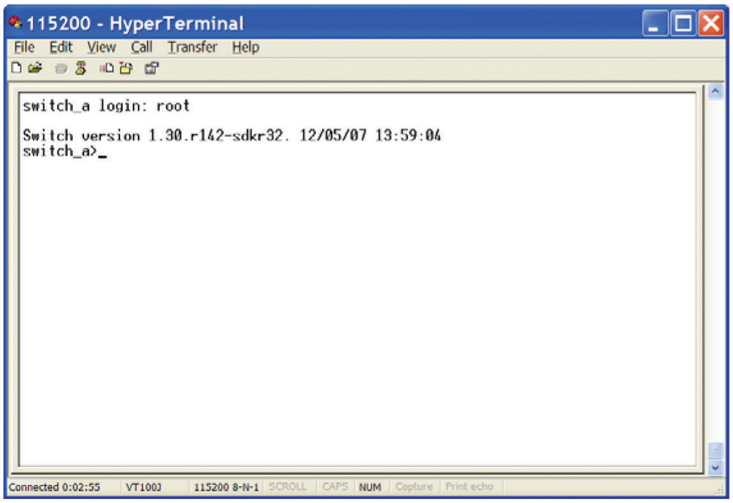
```
switch_a login: _
```

Figure 7-1. Exec mode screen.

Logon to Exec Mode (View Mode)

At the switch_a login: prompt, type in “root” and press <Enter> to logon to Exec Mode (or View Mode).

switch_a login: root


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:02:55
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>_
```

Figure 7-2. View mode screen.

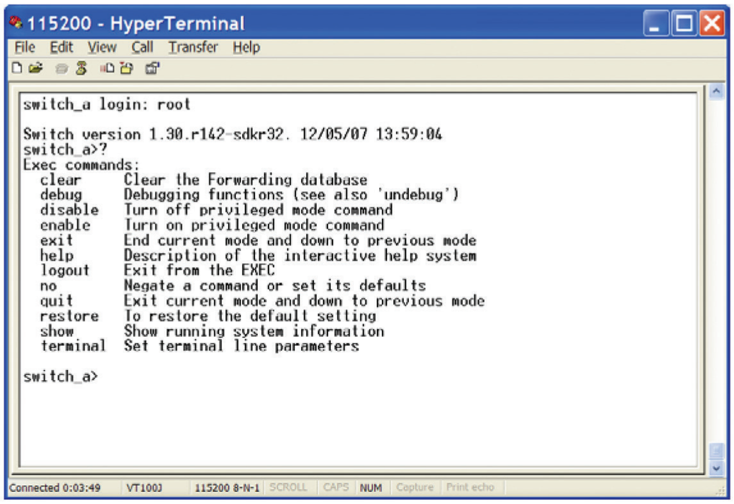
Basic commands

Exec Mode (or View Mode) is the base mode from where users can perform basic commands suchg as: clear, debug, disable, enable, exit, help, logout, no, quit, show, terminal.

The CLI contains a text-based help facility. Access this help by typing in the full or partial command string, then typing a question mark “?”. The CLI displays the command keywords or parameters along with a short description.

At the switch_a> prompt, press <?> to list the above basic commands.

switch_a>?

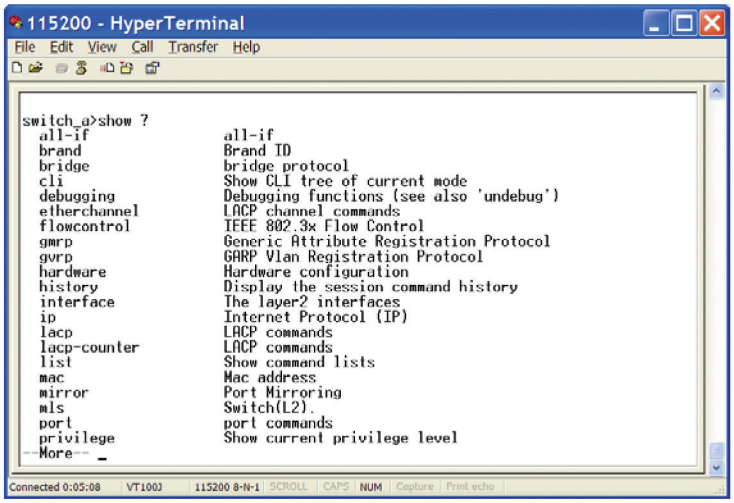

115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:03:49
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>?
Exec commands:
  clear     Clear the Forwarding database
  debug     Debugging functions (see also 'undebug')
  disable   Turn off privileged mode command
  enable    Turn on privileged mode command
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  logout    Exit from the EXEC
  no        Negate a command or set its defaults
  quit      Exit current mode and down to previous mode
  restore   To restore the default setting
  show      Show running system information
  terminal  Set terminal line parameters

switch_a>
```

Figure 7-3.

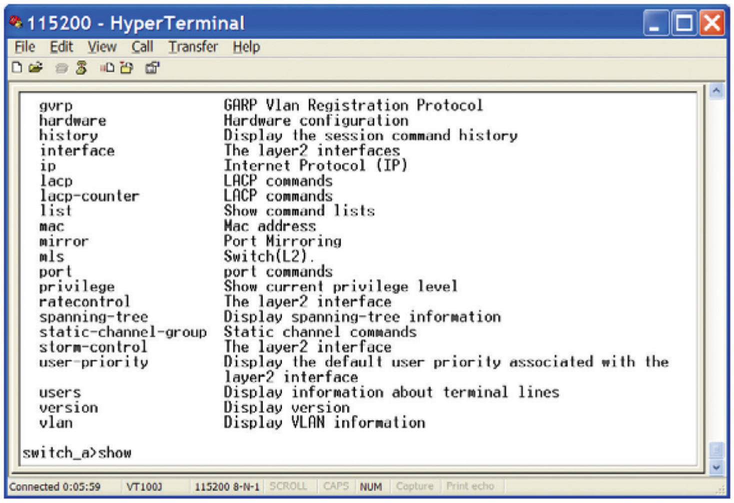
At the switch_a> prompt, type in the full or partial command string then type a question mark “?” to display the command keywords or parameters along with a short description.

switch_a>show ?


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:05:08 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
switch_a>show ?
  all-if                  all-if
  brand                   Brand ID
  bridge                  bridge protocol
  cli                     Show CLI tree of current mode
  debugging               Debugging functions (see also 'undebug')
  etherchannel            LACP channel commands
  flowcontrol             IEEE 802.3x Flow Control
  gmrp                    Generic Attribute Registration Protocol
  gvrp                    GARP Vlan Registration Protocol
  hardware                Hardware configuration
  history                 Display the session command history
  interface               The layer2 interfaces
  ip                      Internet Protocol (IP)
  lacp                    LACP commands
  lacp-counter            LACP commands
  list                    Show command lists
  mac                     Mac address
  mirror                  Port Mirroring
  mls                     Switch(L2).
  port                    port commands
  privilege               Show current privilege level
--More-- _
```

Figure 7-4.


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:05:59 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
  gvrp                    GARP Vlan Registration Protocol
  hardware                Hardware configuration
  history                 Display the session command history
  interface               The layer2 interfaces
  ip                      Internet Protocol (IP)
  lacp                    LACP commands
  lacp-counter            LACP commands
  list                    Show command lists
  mac                     Mac address
  mirror                  Port Mirroring
  mls                     Switch(L2).
  port                    port commands
  privilege               Show current privilege level
  ratecontrol             The layer2 interface
  spanning-tree           Display spanning-tree information
  static-channel-group    Static channel commands
  storm-control           The layer2 interface
  user-priority           Display the default user priority associated with the
                          layer2 interface
  users                   Display information about terminal lines
  version                 Display version
  vlan                    Display VLAN information

switch_a>show
```

Figure 7-5.

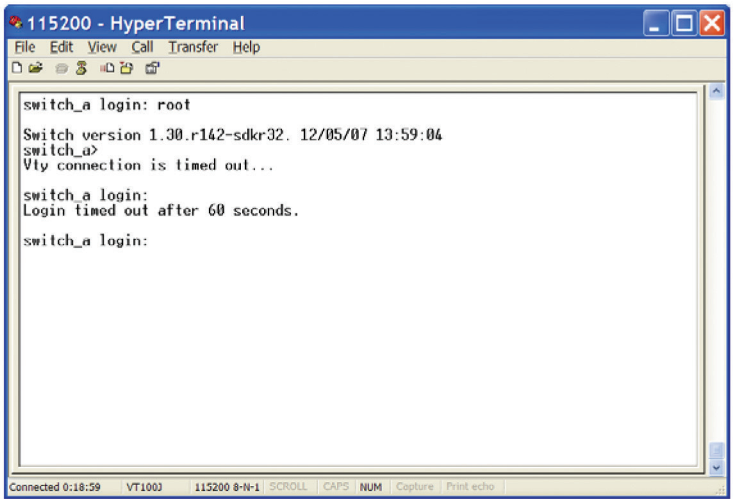
Login timed out

The login session to Exec Mode (or View Mode) has timed out because of an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. The switch_a login: prompt will show on the screen.

Logon back to Exec Mode (View Mode)

At the switch_a login: prompt, type in “root” and press <Enter> to log back on to Exec Mode (or View Mode).

switch_a login: root


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:18:59
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

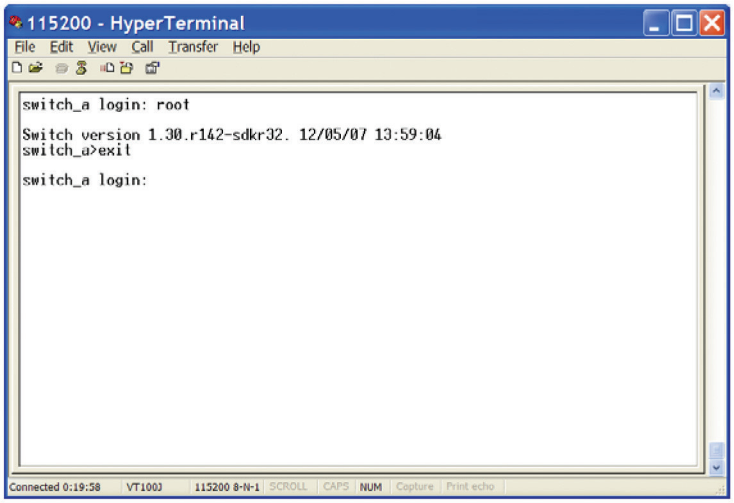
```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>
Vty connection is timed out...

switch_a login:
Login timed out after 60 seconds.

switch_a login:
```

Figure 7-6.

Exit from Exec Mode (View Mode)

At the switch_a> prompt, type in "exit" and press <Enter> to exit from Exec Mode (or View Mode).

```
switch_a>exit
```


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:19:58
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>exit

switch_a login:
```

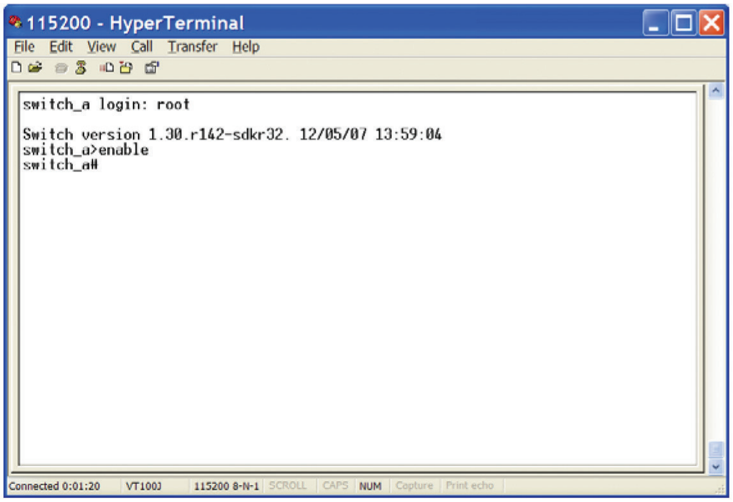
Figure 7-7.

7.1.2 Privileged Exec Mode (Enable Mode)

Logon to Privileged Exec Mode (Enable Mode)

At the switch_a> prompt, type in "enable" and press <Enter> to log on to Privileged Exec Mode (or Enable Mode). The switch_a# prompt will show on the screen.

switch_a>enable


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:01:20
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#
```

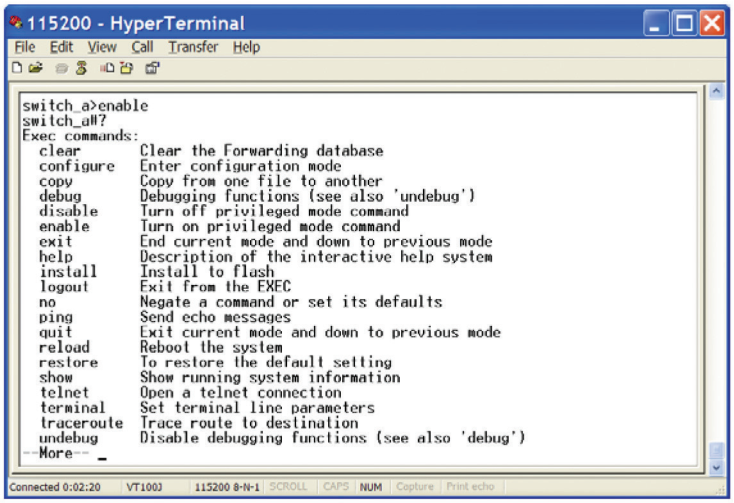
Figure 7-8.

Commands

Privileged Exec Mode (or Enable Mode) allows users to run commands.

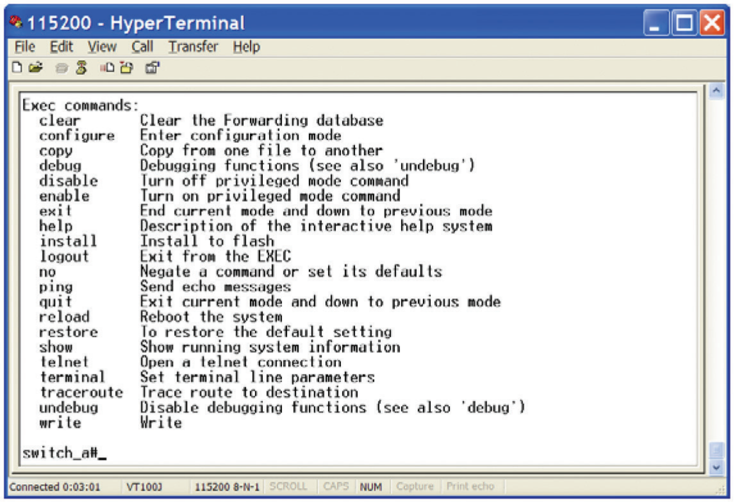
At the switch_a# prompt, press <?> to list the commands.

switch_a#?


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:02:20
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a>enable
switch_a#?
Exec commands:
  clear        Clear the Forwarding database
  configure    Enter configuration mode
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  disable      Turn off privileged mode command
  enable       Turn on privileged mode command
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  install      Install to flash
  logout       Exit from the EXEC
  no           Negate a command or set its defaults
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  reload       Reboot the system
  restore      To restore the default setting
  show         Show running system information
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
  undebug      Disable debugging functions (see also 'debug')
--More-- _
```

Figure 7-9.

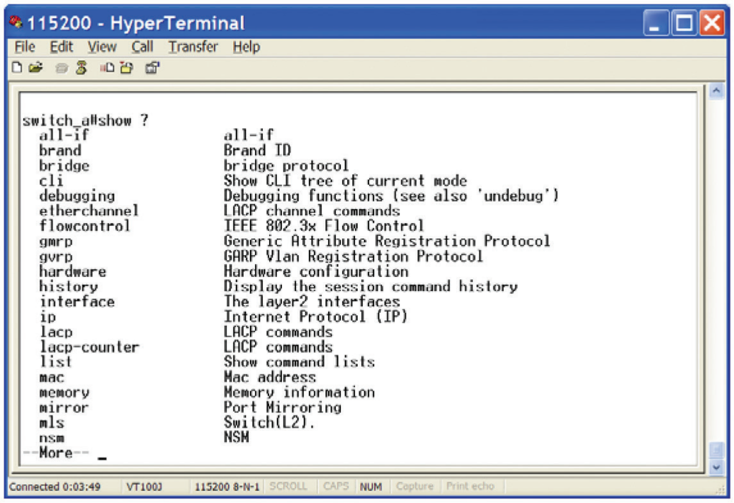

115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:03:01
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
Exec commands:
  clear        Clear the Forwarding database
  configure    Enter configuration mode
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  disable      Turn off privileged mode command
  enable       Turn on privileged mode command
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  install      Install to flash
  logout       Exit from the EXEC
  no           Negate a command or set its defaults
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  reload       Reboot the system
  restore      To restore the default setting
  show         Show running system information
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
  undebug      Disable debugging functions (see also 'debug')
  write        Write

switch_a#_
```

Figure 7-10.

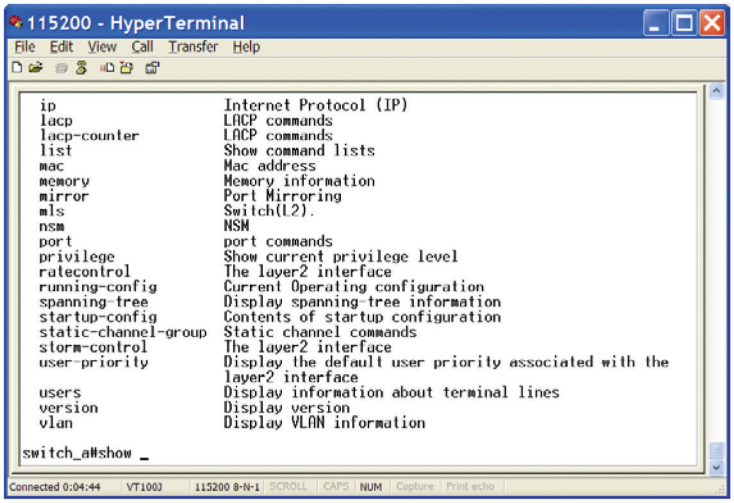
At the switch_a# prompt, type in the full or partial command string, then type a question mark "?" to display the command keywords or parameters along with a short description.

switch_a#show ?


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:03:49
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a#show ?
  all-if                  all-if
  brand                   Brand ID
  bridge                  bridge protocol
  cli                     Show CLI tree of current mode
  debugging               Debugging functions (see also 'undebug')
  etherchannel            LACP channel commands
  flowcontrol             IEEE 802.3x Flow Control
  gmrp                    Generic Attribute Registration Protocol
  gvrp                    GARP Vlan Registration Protocol
  hardware                Hardware configuration
  history                 Display the session command history
  interface               The layer2 interfaces
  ip                      Internet Protocol (IP)
  lacp                    LACP commands
  lacp-counter            LACP commands
  list                    Show command lists
  mac                     Mac address
  memory                  Memory information
  mirror                  Port Mirroring
  mls                     Switch(L2).
  nsm                     NSM
--More-- _
```

Figure 7-11.


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:04:44 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
  ip                      Internet Protocol (IP)
  lacp                    LACP commands
  lacp-counter            LACP commands
  list                    Show command lists
  mac                     Mac address
  memory                  Memory information
  mirror                  Port Mirroring
  mls                     Switch(L2).
  nsm                     NSM
  port                    port commands
  privilege               Show current privilege level
  ratecontrol             The layer2 interface
  running-config          Current Operating configuration
  spanning-tree           Display spanning-tree information
  startup-config          Contents of startup configuration
  static-channel-group    Static channel commands
  storm-control           The layer2 interface
  user-priority           Display the default user priority associated with the
                          layer2 interface
  users                   Display information about terminal lines
  version                 Display version
  vlan                    Display VLAN information

switch_a#show _
```

Figure 7-12.

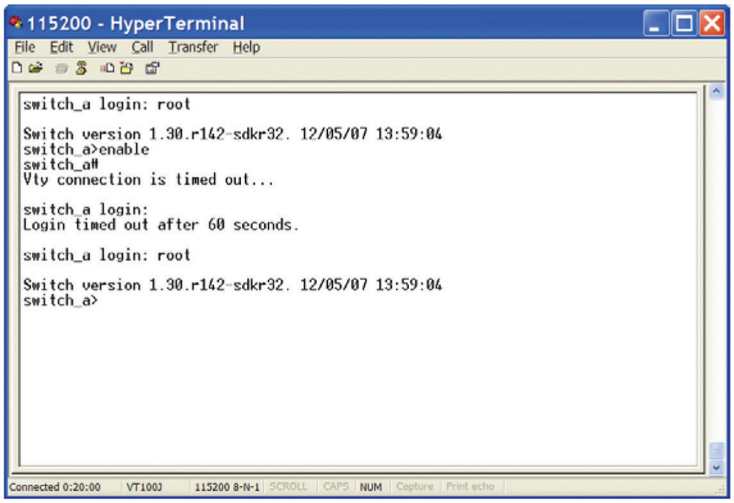
Login timed out

The login session to Privileged Exec Mode (or Enable Mode) has timed out because of an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. The switch_a login: prompt will show on the screen.

Log back on to Exec Mode (View Mode)

At the switch_a login: prompt, type in "root" and press <Enter> to logon back to Exec Mode (or View Mode).

switch_a login: root


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:20:00 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

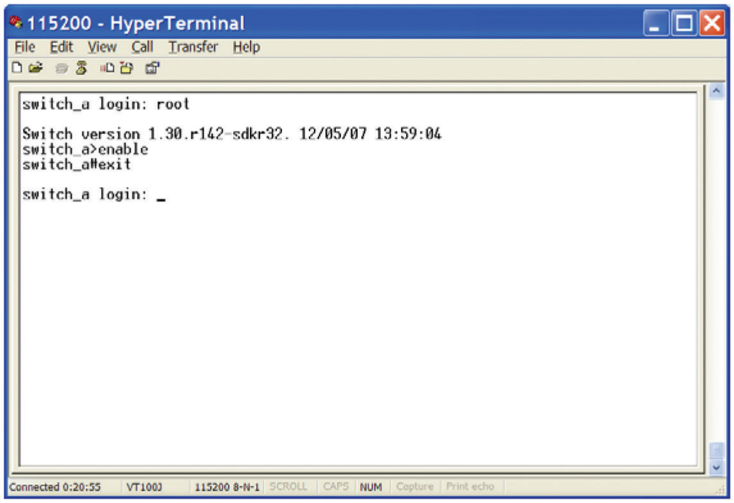
```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#
Vty connection is timed out...

switch_a login:
Login timed out after 60 seconds.

switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>
```

Figure 7-13.

Exit from Privileged Exec Mode (or Enable Mode)

At the switch_a# prompt, type in "exit" and press <Enter> to exit from Privileged Exec Mode (or Enable Mode).

switch_a#exit


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:20:55 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#exit

switch_a login: _
```

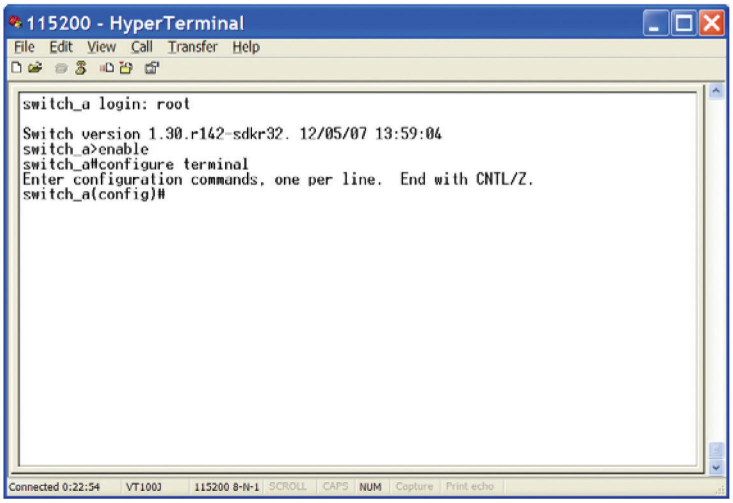
Figure 7-14.

7.1.3 Configure Mode (Configure Terminal Mode)

Logon to Configure Mode (Configure Terminal Mode)

At the switch_a# prompt, type in "configure terminal" and press <Enter> to log on to Configure Mode (or Configure Terminal Mode). The switch_a(config)# prompt will show on the screen.

switch_a#configure terminal


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:22:54 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_a(config)#
```

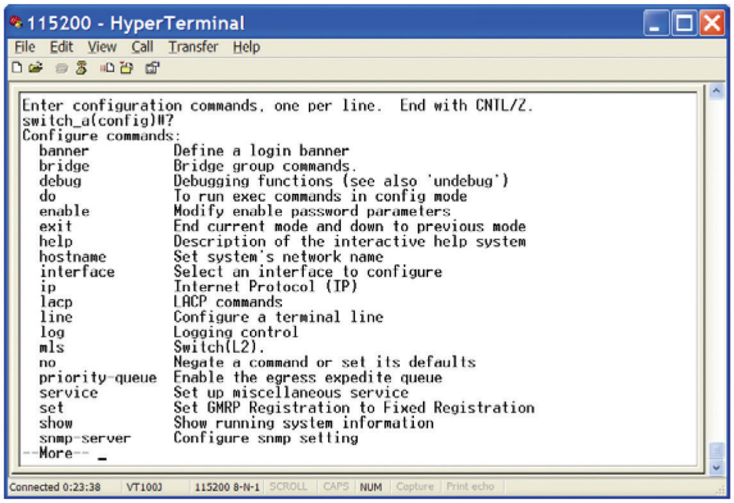
Figure 7-15.

Commands

Configure Mode (or Configure Terminal Mode) serves as a gateway into the modes as following.

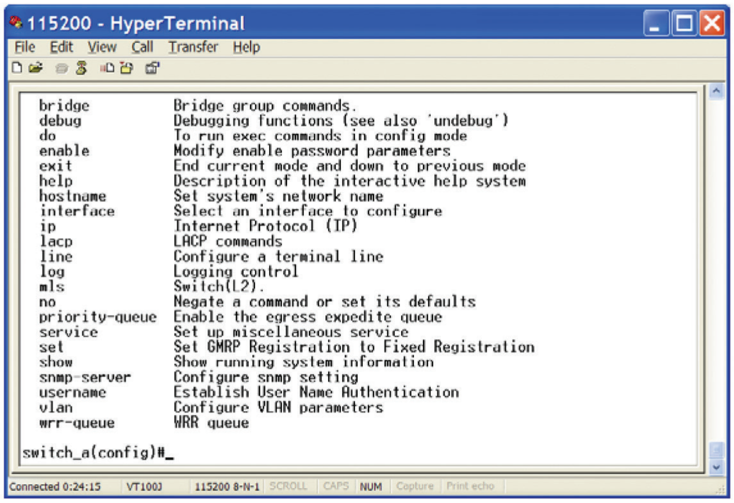
At the switch_a(config)# prompt, press <?> to list the commands.

switch_a(config)#?


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:23:38 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
Enter configuration commands, one per line.  End with CNTL/Z.
switch_a(config)#?
Configure commands:
  banner           Define a login banner
  bridge           Bridge group commands.
  debug            Debugging functions (see also 'undebug')
  do               To run exec commands in config mode
  enable           Modify enable password parameters
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  hostname         Set system's network name
  interface        Select an interface to configure
  ip               Internet Protocol (IP)
  lacp             LACP commands
  line             Configure a terminal line
  log              Logging control
  mls              Switch(L2).
  no               Negate a command or set its defaults
  priority-queue   Enable the egress expedite queue
  service          Set up miscellaneous service
  set              Set GMRP Registration to Fixed Registration
  show             Show running system information
  snmp-server      Configure snmp setting
--More-- _
```

Figure 7-16.

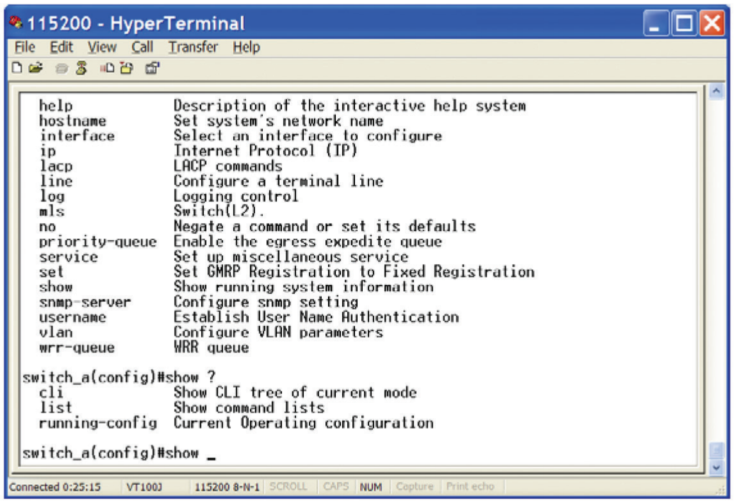

115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:24:15 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
  bridge           Bridge group commands.
  debug            Debugging functions (see also 'undebug')
  do               To run exec commands in config mode
  enable           Modify enable password parameters
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  hostname         Set system's network name
  interface        Select an interface to configure
  ip               Internet Protocol (IP)
  lacp             LACP commands
  line             Configure a terminal line
  log              Logging control
  mls              Switch(L2).
  no               Negate a command or set its defaults
  priority-queue   Enable the egress expedite queue
  service          Set up miscellaneous service
  set              Set GMRP Registration to Fixed Registration
  show             Show running system information
  snmp-server      Configure snmp setting
  username         Establish User Name Authentication
  vlan             Configure VLAN parameters
  wrr-queue        WRR queue

switch_a(config)#_
```

Figure 7-17.

At the switch_a(config)# prompt, type in the full or partial command string, then type a question mark "?" to display the command keywords or parameters along with a short description.

switch_a(config)#show ?


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:25:15 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
  help            Description of the interactive help system
  hostname        Set system's network name
  interface       Select an interface to configure
  ip              Internet Protocol (IP)
  lacp            LACP commands
  line            Configure a terminal line
  log             Logging control
  mls             Switch(L2).
  no              Negate a command or set its defaults
  priority-queue  Enable the egress expedite queue
  service         Set up miscellaneous service
  set             Set GMRP Registration to Fixed Registration
  show            Show running system information
  snmp-server     Configure snmp setting
  username        Establish User Name Authentication
  vlan            Configure VLAN parameters
  wrr-queue       WRR queue

switch_a(config)#show ?
  cli             Show CLI tree of current mode
  list            Show command lists
  running-config  Current Operating configuration

switch_a(config)#show _
```

Figure 7-18.

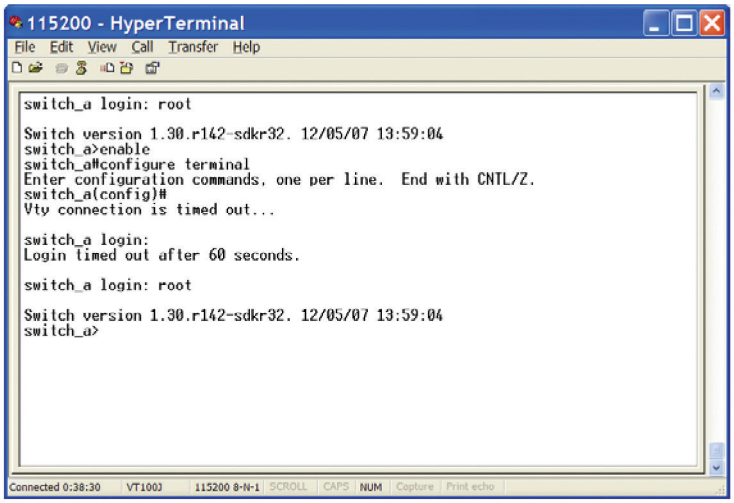
Login timed out

The login session to Configure Mode (or Configure Terminal Mode) has timed out because of an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. And the switch_a login: prompt will show on the screen.

Logon back to Exec Mode (View Mode)

At the switch_a login: prompt, type in "root" and press <Enter> to log back on to Exec Mode (or View Mode).

switch_a login: root


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:38:30 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

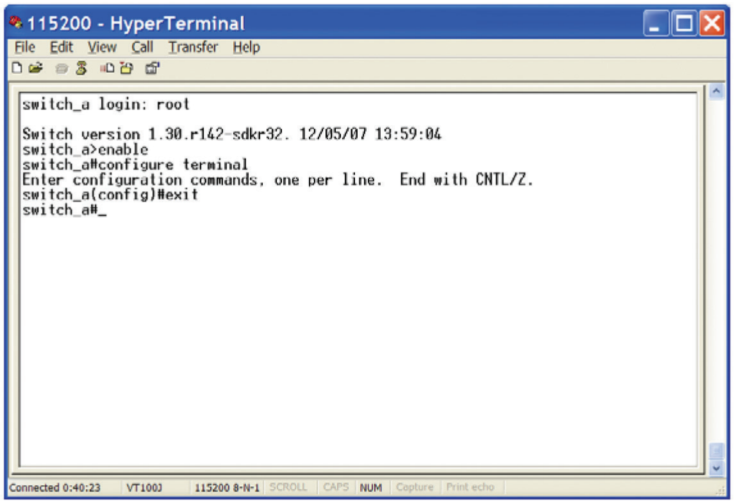
```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_a(config)#
Vty connection is timed out...

switch_a login:
Login timed out after 60 seconds.

switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>
```

Figure 7-19.

Exit from Configure Mode (or Configure Terminal Mode)

At the switch_a(config)# prompt, type in "exit" and press <Enter> to exit from Configure Mode (or Configure Terminal Mode).

switch_a(config)#exit


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 0:40:23
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a login: root

Switch version 1.30.r142-sdkr32. 12/05/07 13:59:04
switch_a>enable
switch_a#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_a(config)#exit
switch_a#_
```

Figure 7-20.

7.2 System

System Information, System Name/Password, IP Address, Save Configuration, Firmware Upgrade, Reboot, Logout, User Account, User Privilege

System Name/Password

System Name:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use hostname command to set or change the network server name.

Use the no hostname command to disable this function.

3. Command Syntax:

(no) hostname HOSTNAME

HOSTNAME specifies the network name of the system.

4. Example:

The following example sets the hostname to switch, and shows the change in the prompt:

switch_a(config)#hostname switch

switch(config)#

Password:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use the enable password command to modify or create a password to be used when entering the Enable mode.

3. Command Syntax:

```
enable password PASSWORD
```

PASSWORD specifies the new password of the system.

4. Example:

The following example sets the new password mypasswd to switch:

```
switch_a(config)#enable password mypasswd
switch_a(config)#
```

IP Address

IP Address/IP Subnet Mask:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip address command to set the IP address of an interface.

Use the no ip address command to remove the IP address from an interface.

3. Command Syntax:

```
ip address IP-ADDRESS
no ip address IP-ADDRESS
no ip address
```

IP-ADDRESS A.B.C.D/M specifies the IP address and prefix length of an interface.

M specifies IP subnet mask, 8: 255.0.0.0, 16:255.255.0.0, 24: 255.255.255.0.

4. Example:

The following example sets the new IP address 192.168.1.10 and new IP subnet mask 255.255.255.0 to switch:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip address 192.168.1.10/24
switch_a(config-if)#
```

DHCP Client:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use get ip dhcp enable command to get IP address through DHCP server.

Use the no get ip dhcp enable command to cancel the IP address which got through DHCP server.

3. Command Syntax:

```
(no) get ip dhcp enable
```

4. Example:

The following example gets IP address through DHCP server:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#get ip dhcp enable
switch_a(config-if)#
```

Default Gateway:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use ip default-gateway command to set the IP address of the default gateway.

Use the no ip default-gateway command to remove the IP address of the default gateway.

3. Command Syntax:

```
ip default-gateway IP-ADDRESS
no ip default-gateway
```

IP-ADDRESS A.B.C.D specifies the IP address of the default gateway.

4. Example:

The following example sets the default gateway 192.168.1.254 to switch:

```
switch_a(config)#ip default-gateway 192.168.1.254
switch_a(config)#
```

DNS Server:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use ip dns command to set the IP address of the DNS server.

Use the no ip dns command to remove the IP address of the DNS server.

3. Command Syntax:

ip dns IP-ADDRESS

no ip dns

IP-ADDRESS A.B.C.D specifies the IP address of the DNS server.

4. Example:

The following example sets the DNS server 192.168.1.100 to switch:

```
switch_a(config)#ip dns 192.168.1.100
switch_a(config)#
```

Save Configuration

Load config from TFTP server:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use install image command to load configuration file from tftp server to switch.

3. Command Syntax:

install image IP-ADDRESS WORD

IP-ADDRESS specifies the IP address of tftp server.

WORD specifies the file name to be loaded to switch.

4. Example:

The following example specifies upgrading firmware (file name: flash.tgz) from tftp server (IP address: 192.168.1.100) to switch:

```
switch_a#install image 192.168.1.100 flash.tgz
switch_a#
```

Load config to TFTP server:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use write config-file command to back up the configuration file to tftp server.

3. Command Syntax:

```
write config-file IP-ADDRESS
```

IP-ADDRESS specifies the IP address of the tftp server.

4. Example:

The following example backs up the configuration file to the tftp server (IP address: 192.168.1.20):

```
switch_a#write config-file 192.168.1.20
switch_a#
```

Save Configuration:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use copy running-config startup-config command to write configurations to the file to be used at startup. This is the same as the write memory command.

3. Command Syntax:

```
copy running-config startup-config
```

4. Example:

The following example specifies writing configurations to the file to be used at startup to switch:

```
switch_a#copy running-config startup-config
switch_a#
```

Restore Default:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use restore default command to restore the default setting of the switch.

3. Command Syntax:

```
restore default
```

4. Example:

The following example restores the default setting of the switch:

```
switch_a#restore default
switch_a#
```

Auto Save:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable auto save configuration function. The configuration will automatically be saved at every configured interval when this command is enabled. Use the no form of this command to disable this feature.

3. Command Syntax:

```
service auto-config enable
no service auto-config enable
```

4. Example:

The following example enables or disables auto save the configuration to the switch:

```
switch_a(config)#service auto-config enable
switch_a(config)#no service auto-config enable
switch_a(config)#
```

Auto Save Interval (5–65536 sec):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the interval when the configuration will automatically be saved. The range of interval value is from 5 to 65535. The default value is 30 seconds.

3. Command Syntax:

```
service auto-config interval WORD
```

WORD specifies the interval value.

4. Example:

The following example sets the interval WORD (10) when the configuration will be automatically saved to switch:

switch_a(config)#service auto-config interval 10

switch_a(config)#

Firmware Upgrade

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

switch_a#

2. Usage:

Use install image command to upgrade firmware from tftp server to switch.

3. Command Syntax:

install image IP-ADDRESS WORD

IP-ADDRESS specifies the IP address of tftp server.

WORD specifies the file name to be upgraded to switch.

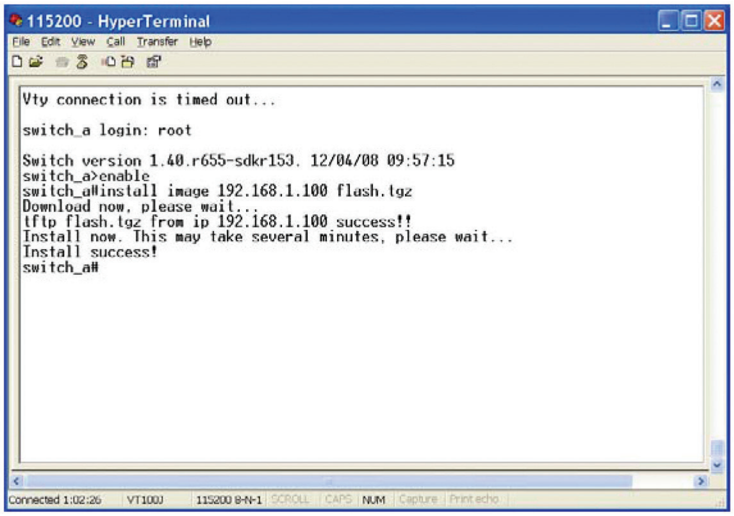
4. Example:

The following example specifies upgrading firmware (file name: flash.tgz) from the tftp server (IP address: 192.168.1.100) to the switch:

switch_a#install image 192.168.1.100 flash.tgz

switch_a#

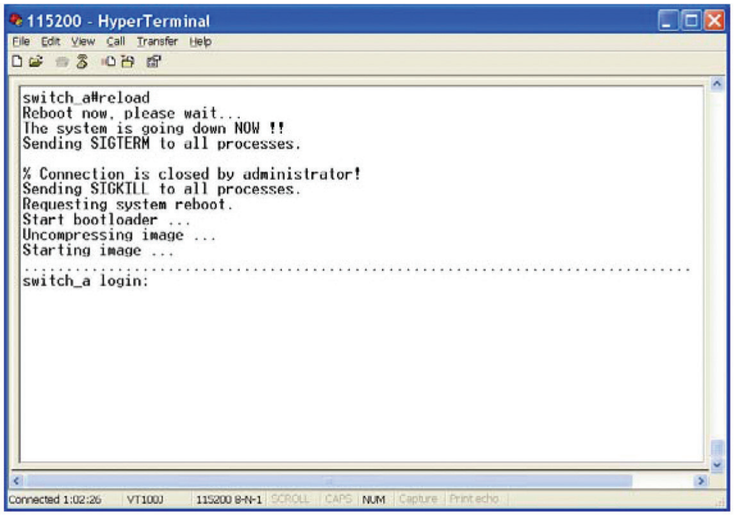
Follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time.


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 1:02:26 VT100J 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
Vty connection is timed out...

switch_a login: root

Switch version 1.40.r655-sdkr153. 12/04/08 09:57:15
switch_a>enable
switch_a#install image 192.168.1.100 flash.tgz
Download now, please wait...
tftp flash.tgz from ip 192.168.1.100 success!!
Install now. This may take several minutes, please wait...
Install success!
switch_a#
```

Figure 7-21.

At the "switch_a#" prompt just type in "reload" and press <Enter> to reboot the switch after completing the upgrade process.


115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 1:02:26
VT100J
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
switch_a#reload
Reboot now, please wait...
The system is going down NOW !!
Sending SIGTERM to all processes.

% Connection is closed by administrator!
Sending SIGKILL to all processes.
Requesting system reboot.
Start bootloader ...
Uncompressing image ...
Starting image ...
................................................................................
switch_a login:
```

Figure 7-22.

Reboot

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

switch_a#

2. Usage:

Use reload command to restart switch.

3. Command Syntax:

reload

4. Example:

The following example specifies restarting switch:

switch_a#reload

switch_a login:

Logout

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

switch_a>

switch_a#

2. sUsage:

Use logout command to exit from the Exec mode or Privileged Exec mode.

3. Command Syntax:

logout

4. Example:

The following example specifies to exit from the Exec mode or Privileged Exec mode.

```
switch_a>logout
switch_a login:
```

User Account

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the privilege level and set a password to user who needs to access the Switch at this level.

Use the no username command to disable this function.

3. Command Syntax:

```
username WORD privilege (admin | operator | technician) password LINE
username WORD privilege (admin | operator | technician) password 8 LINE
no username WORD
```

WORD User name.

- Specifies the password will be hidden.

LINE User password string.

4. Example:

The following example sets the privilege level operator and password 111111111111 for user operator:

```
switch_a(config)#username operator operator password 111111111111
switch(config)#
```

7.3 Diagnostics

Utilization, System Log, Remote Logging, ARP Table, Route Table, Alarm Setting

Utilization

CPU Utilization:

1. Command Mode: Exec mode

Logon to Exec Mode (View Mode).

The switch_a> prompt will show on the screen.

```
switch_a>
```

2. Usage:

Use the show cpu-usage command to show the CPU usage.

3. Command Syntax:

```
show cpu-usage
```

4. Example:

The following example shows the CPU usage:

```
switch_a>show cpu-usage
```

Memory Utilization:

1. Command Mode: Exec mode

Logon to Exec Mode (View Mode).

The switch_a> prompt will show on the screen.

```
switch_a>
```

2. Usage:

Use the show memory-usage command to show the memory usage.

3. Command Syntax:

```
show memory-usage
```

4. Example:

The following example shows the memory usage:

```
switch_a>show memory-usage
```

System Log

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use the show system-log command to show the system log.

3. Command Syntax:

show system-log

4. Example:

The following example shows the system log of the switch:

```
switch_a>show system-log
```

Remote Logging

Remote Logging:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable logging messages sent to syslog servers.

Use the no parameter with this command to disable the logging of messages that are sent to syslog servers.

3. Command Syntax:

(no) remote-log enable

4. Example:

The following example enables remote logging:

```
switch_a(config)#remote-log enable
switch_a(config)#
```

Add Syslog Server:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the logging of messages that are sent to remote syslog servers.

3. Command Syntax:

remote-log del A.B.C.D

A.B.C.D Specifies the IP address of the remote syslog server.

4. Example:

The following example deletes a remote syslog server (IP address: **192.168.1.100**) for the switch:

```
switch_a(config)#remote-log del 192.168.1.100
switch_a(config)#
```

ARP Table

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use show arp-table command to view ARP Table.

3. Command Syntax:

show arp-table

4. Example:

The following example shows the ARP Table of the switch:

```
switch_a#show arp-table
```

Route Table

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use the show route-table command to view Route Table.

3. Command Syntax:

show route-table

4. Example:

The following example shows the Route Table of the switch:

```
switch_a#show route-table
```

Alarm Setting

Alarm-trigger if:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable alarm trigger on interface.

3. Command Syntax:

```
(no) alarm-trigger if INTERFACE
```

INTERFACE specifies the interface.

4. Example:

The following example enables alarm trigger on interface “fe1” to switch:

```
switch_a(config)#alarm-trigger if fe1
switch_a(config)#
```

Alarm-trigger power:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable alarm trigger of power source.

3. Command Syntax:

```
(no) alarm-trigger power POWER
```

POWER specifies the power source.

4. Example:

The following example enables alarm trigger of power “1” to switch:

```
switch_a(config)#alarm-trigger power 1
switch_a(config)#
```

7.4 Port

Configuration, Port Status, Rate Control, RMON Statistics, Per Port VLAN Activities

Configuration

Port Name:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use the portname command to specify the ascii name of port.

Use the no portname to cancel the ascii name of port.

3. Command Syntax:

```
portname LINE
(no) portname
```

LINE specifies the ascii name of port.

4. Example:

The following example shows the use of the portname command to specify the ascii name fe1 for the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#portname fe1
switch_a(config-if)#
```

Admin Setting:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use the shutdown command to shut down the selected interface.

Use the no shutdown to disable this function.

3. Command Syntax:

(no) shutdown

4. Example:

The following example shows the use of the shutdown command to shut down the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#shutdown
switch_a(config-if)#
```

Duplex:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use duplex command to specify the duplex mode to be used for each interface.

Use the no duplex to disable this function.

3. Command Syntax:

(no) duplex MODE

MODE specifies the duplex mode: auto, full, half.

4. Example:

The following example shows the use of duplex MODE (full) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#duplex full
switch_a(config-if)#
```

Flow control:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use flowcontrol on command to enable flow control, and configure the flow control mode for the port.

Use the no flowcontrol to disable this function.

3. Command Syntax:

```
flowcontrol on
no flowcontrol
```

4. Example:

The following example shows the use of flowcontrol on to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#flowcontrol on
switch_a(config-if)#
```

Port Status

Port Status:

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use the show interface command to display interface configuration and status.

3. Command Syntax:

```
show interface IFNAME
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

4. Example:

The following example shows the use of show interface to display interface configuration and status of the interface fe1 (port 1):

```
switch_a>show interface fe1
```

Alarm Situation:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use the show sfp-alarm-trigger command to show the information of SFP alarm trigger including temperature, Vcc, Tx_bias, Tx_pow and Rx_pow.

3. Command Syntax:

```
show sfp-alarm-trigger IFNAME
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

4. Example:

The following example shows the use of show sfp-alarm-trigger to display the information of SFP alarm trigger of the interface ge1 (port G1):

```
switch_a#show sfp-alarm-trigger ge1
```

Temperature Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set temperature alarm (warning) threshold for SFP transceiver.

3. Command Syntax:

```
sfp set-temp IFNAME high-alarm high-warning low alarm low warning LEVEL
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

LEVEL Threshold value -128 ~ 128 .

4. Example:

The following example sets high temperature alarm threshold 100 for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-temp ge1 high-alarm 100
switch_a(config)#
```

Voltage Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set voltage alarm (warning) threshold for SFP transceiver.

3. Command Syntax:

```
sfp set-vcc IFNAME high-alarm high-warning low alarm low warning LEVEL
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

LEVEL Threshold value 0 ~ 6.55 volts.

4. Example:

The following example sets high voltage alarm threshold 6 volts for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-vcc ge1 high-alarm 6
switch_a(config)#
```

Tx-bias Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set transmitter laser bias alarm (warning) threshold for SFP transceiver.

3. Command Syntax:

```
sfp set-tx-bias IFNAME high-alarm high-warning low alarm low warning LEVEL
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

LEVEL Threshold value 0 ~ 131 mA.

4. Example:

The following example sets high transmitter laser bias alarm threshold 131 mA for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-tx-bias ge1 high-alarm 131
switch_a(config)#
```

Tx-pow Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set transmitted output power alarm (warning) threshold for SFP transceiver.

3. Command Syntax:

```
sfp set-tx-pow IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

LEVEL Threshold value -30–8.16 dbm.

4. Example:

The following example sets high transmitted output power alarm threshold 8.16 dbm for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-tx-pow ge1 high-alarm 8.16
switch_a(config)#
```

Rx-pow Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set received optical power alarm (warning) threshold for SFP transceiver.

3. Command Syntax:

```
sfp set-rx-pow IFNAME high-alarm high-warning low alarm low warning LEVEL
```

IFNAME specifies the name of the interface for which status and configuration information is desired.

LEVEL Threshold value -30 ~ 8.16 dbm.

4. Example:

The following example sets high received optical power alarm threshold 8.16 dbm for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-rx-pow ge1 high-alarm 8.16
switch_a(config)#
```

Rate Control

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to specify the ingress/egress rate to be used for each interface. The bandwidth value is in bits.

Use the no parameter with this command to remove the ingress/egress rate to be used for each interface.

3. Command Syntax:

```
(no) rate-control ingress/egress VALUE
```

VALUE

<1-10000000000 bits> (usable units: k, m, g)

<1-999>k|m for 1 to 999 kilo bits or mega bits.

1g for 1 giga bits.

4. Example:

The following example shows the use of rate-control ingress VALUE (10 mega bits) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#rate-control ingress 10m
switch_a(config-if)#
```

RMON Statistics

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use the show interface statistics command to display RMON statistics of interface.

3. Command Syntax:

show interface statistics IFNAME

IFNAME specifies the name of the interface for which RMON statistics is desired.

4. Example:

The following example shows the use of show interface statistics to display RMON statistics of the interface fe1 (port 1):

```
switch_a>show interface statistics fe1
```

Per Port VLAN Activities

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use show vlan command to display information about a particular VLAN by specifying the VLAN ID.

3. Command Syntax:

show vlan <2-4094>

<2-4094> VLAN ID.

4. Example:

The following is an output of show vlan command displaying information about VLAN 2:

```
switch_a>show vlan 2
```

7.5 Switching

Bridging, Loopback Detect, Static MAC Entry, Port Mirroring, Link State Tracking, PoE, PoE Scheduling

Bridging

Aging Time (seconds):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist till this specified time.

3. Command Syntax:

```
Bridge GROUP ageing-time AGEINGTIME
no bridge GROUP ageing-time
```

Group = <1-1> The ID of the bridge-group that this ageing time is for.

AGEINGTIME = <10-1000000> The number of seconds of persistence.

4. Example:

The following example sets the new AGEINGTIME (1000) to bridge GROUP (1):

```
switch_a(config)#bridge 1 ageing-time 1000
switch_a(config)#
```

Threshold level (0-100):

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use storm-control level command to specify the rising threshold level for broadcasting, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

3. Command Syntax:

```
storm-control level LEVEL
```

LEVEL <0-100> specifies the percentage of the threshold; percentage of the maximum speed (pps) of the interface.

4. Example:

The following example shows setting storm-control level LEVEL (30) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control level 30
switch_a(config-if)#
```

Broadcast:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use storm-control broadcast enable command to enable broadcast traffic.

Use no storm-control broadcast command to disable broadcast traffic.

3. Command Syntax:

```
storm-control broadcast enable
no storm-control broadcast
```

4. Example:

The following example shows setting storm-control broadcast enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control broadcast enable
switch_a(config-if)#
```

Multicast:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use storm-control multicast enable command to enable multicast traffic.

Use no storm-control multicast command to disable multicast traffic.

3. Command Syntax:

storm-control multicast enable

no storm-control multicast

4. Example:

The following example shows setting storm-control multicast enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control multicast enable
switch_a(config-if)#
```

DLF:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use storm-control dlf enable command to enable destination lookup failure traffic.

Use no storm-control dlf command to disable destination lookup failure traffic.

3. Command Syntax:

storm-control dlf enable

no storm-control dlf

dlf destination lookup failure

4. Example:

The following example shows setting storm-control dlf enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control dlf enable
switch_a(config-if)#
```

Port isolation:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use port-isolation enable command to enable port isolation.

Use port-isolation disable command to disable port isolation.

3. Command Syntax:

```
port-isolation (enable | disable)
```

4. Example:

The following example enables port-isolation to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#port-isolation enable
switch_a(config-if)#
```

Loopback Detect

LoopBack Detect:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable a loopback detection on a port interface.

3. Command Syntax:

```
bridge GROUP loopback-detect (enable disable)
```

GROUP <1-1> Bridge-group ID used for bridging.

enable Enables a loopback detection on a port interface.

disable Disables a loopback detection on a port interface.

4. Example:

The following example enables a loopback detection for bridge GROUP (1):

```
switch_a(config)#bridge 1 loopback-detect enable
switch_a(config)#
```

LoopBack Detect Action:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to configure action while loopback detected.

3. Command Syntax:

```
bridge GROUP loopback-detect action (errdisable | none (default))
```

GROUP <1-1> Bridge-group ID used for bridging.

errdisable Enable error disable LoopBack Detect Action on a port interface.

none Disable error disable LoopBack Detect Action on a port interface.

4. Example:

The following example enables error disable LoopBack Detect Action for bridge GROUP (1):

```
switch_a(config)#bridge 1 loopback-detect action errdisable
switch_a(config)#
```

Error Disable Recovery:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the error disable recovery time interval. The range of interval value is from 0 to 65535. And the default value is 0 second (no recovery).

3. Command Syntax:

```
bridge GROUP loopback-detect errdisable-recovery <0-65535>
```

GROUP <1-1> Bridge-group ID used for bridging.

<0-65535> The error disable recovery time in seconds.

4. Example:

The following example sets error disable recovery time 1 second for bridge GROUP (1):

```
switch_a(config)#bridge 1 loopback-detect errdisable-recovery 1
switch_a(config)#
```

Interval:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the loopback detect interval time. The range of interval value is from 1 to 65535. And the default value is 1 second.

3. Command Syntax:

```
bridge GROUP loopback-detect interval <1-65535>
```

GROUP <1-1> Bridge-group ID used for bridging.

<1–65535> The loopback detect interval time in seconds.

4. Example:

The following example sets loopback detect interval time 10 seconds for bridge GROUP (1):

```
switch_a(config)#bridge 1 loopback-detect interval 10
switch_a(config)#
```

Loopback Detect (Port Interface):

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enable loopback detect for port interface.

Use the no parameter with this command to disable loopback detect for port interface.

3. Command Syntax:

```
loopback-detect port enable
no loopback-detect port enable
```

4. Example:

The following example enables loopback detect for port fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#loopback-detect port enable
switch_a(config-if)#
```

Static MAC Entry

Static-MAC-Entry Forward:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to statically configure a bridge entry to forward matching frames.

3. Command Syntax:

```
bridge GROUP address MAC forward IFNAME VLANID
no bridge GROUP address MAC forward IFNAME VLANID
```

GROUP <1-1> Bridge-group ID used for bridging.

MAC the Media Access Control (MAC) address in the HHHH.HHHH.HHHH format.

IFNAME the interface on which the frame comes in.

VLANID The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.

4. Example:

The following example configures a bridge GROUP (1) to forward matching frames (MAC address 2222.2222.2222) to the interface fe1 (port 1) in vlan VLANID (2):

```
switch_a(config)#bridge 1 address 2222.2222.2222 forward fe1 vlan 2
switch_a(config)#
```

Static-MAC-Entry Discard:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to statically configure a bridge entry to discard matching frames in a particular VLAN.

3. Command Syntax:

```
bridge GROUP address MAC discard vlan VLANID
no bridge GROUP address MAC discard vlan VLANID
```

GROUP <1-1> Bridge-group ID used for bridging.

MAC the Media Access Control (MAC) address in the HHHH.HHHH.HHHH format.

VLANID The VID of the VLAN on the bridge <1-4094>.

4. Example:

The following example configures a bridge GROUP (1) to discard matching frames (MAC address 2222.2222.2222) in vlan VLANID (1):

```
switch_a(config)#bridge 1 address 2222.2222.2222 discard vlan 1
switch_a(config)#
```

Port Mirroring

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to define a mirror source port and its direction.

Use the no parameter with this command to disable port mirroring by the destination port on the specified source port.

3. Command Syntax:

```
mirror interface SOURCEPORT direction SNOOPDIRECTION
no mirror interface SOURCEPORT
```

SOURCEPORT Name of the Source interface to be used.

SNOOPDIRECTION [both|receive|transmit]

both Specifies mirroring of traffic in both directions.

receive Specifies mirroring of received traffic.

transmit Specifies mirroring of transmitted traffic.

4. Example:

The following example enables port mirroring by the destination port fe1 (port 1) on the specified source port fe2 (port 2):

```
switch_a(config)#interface fe1
switch_a(config-if)#mirror interface fe2 direction both
switch_a(config-if)#
```

Link State Tracking

Group Setting:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable link state tracking for the group.

Use the no parameter with this command to disable link state tracking for the group.

3. Command Syntax:

```
(no) link state track <1-10>
```

<1-10> Link state group number.

4. Example:

The following example enables link state tracking for the group 1:

```
switch_a(config)#link state track 1
switch_a(config)#
```

Port Setting:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enable link state tracking for the port.

Use the no parameter with this command to disable link state tracking for the port.

3. Command Syntax:

(no) link state group <1-10> (downstream upstream)

<1-10> Link state group number.

4. Example:

The following example enables downstream link state tracking of port fe1 (port 1) for the group 1:

```
switch_a(config)#interface fe1
switch_a(config-if)# link state group 1 downstream
switch_a(config-if)#
```

PoE (for LEH1000 Series Switches only)

System Power Budget:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the power budget (Watts) to be set to Switch.

3. Command Syntax:

poe system-power-budget LEVEL

LEVEL <1-800> specifies the power budget (Watts) to be set to Switch.

4. Example:

The following example sets new power budget 246 Watts to Switch:

```
switch_a(config)#poe system-power-budget 246
switch_a(config)#
```

Enable Mode:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use poe enable command to enable this port to discover Powered Device (PD) connected to this port.

Use the no poe enable to disable this function.

3. Command Syntax:

```
(no) poe enable
```

4. Example:

The following example shows the use of poe enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe enable
switch_a(config-if)#
```

Power Limit by Classification:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use poe power-classification enable command to enable this port to provide power to PD according to classification of maximum power range used by PD.

Use the no poe power-classification enable to disable this function.

3. Command Syntax:

```
(no) poe power-classification enable
```

4. Example:

The following example shows the use of poe power-classification enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-classification enable
switch_a(config-if)#
```

Fixed Power Limit (W):

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to specify the fixed power limit for this port to provide power to PD.

3. Command Syntax:

```
poe fixed-power-limit LEVEL
```

LEVEL <1-15.4> specifies the fixed power limit (Watts) for this port to provide power to PD.

4. Example:

The following example sets new fixed power limit 15 Watts to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe fixed-power-limit 15
switch_a(config-if)#
```

Power Priority:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to specify the power priority to this port.

3. Command Syntax:

```
poe power-priority PRIORITY
```

PRIORITY specifies high, medium, low power priority for this port.

4. Example:

The following example sets high power priority to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-priority high
switch_a(config-if)#
```

Power Down Alarm:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use poe power-down-alarm enable command to enable power down alarm to this port.

Use the no poe power-classification enable to disable this function.

3. Command Syntax:

```
(no) poe power-down-alarm enable
```

4. Example:

The following example shows the use of poe power-down-alarm enable to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-down-alarm enable
switch_a(config-if)#
```

PoE Scheduling (for LEH1000 Series Switches)

PoE Schedule:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enble PoE scheduling to this port.

3. Command Syntax:

poe scheduling enable

4. Example:

The following example enables PoE scheduling to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe scheduling enable
switch_a(config-if)#
```

PoE Schedule:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set PoE scheduling to this port.

3. Command Syntax:

poe schedule-time DAY HOUR

DAY <0-6> specifies Sunday ~ Saturday to Switch.

HOUR <0-23> specifies hours to Switch.

no poe schedule-time DAY

4. Example:

The following example sets PoE scheduling to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe schedule-time 3 0-10,12,14-20, 22-23
switch_a(config-if)#
```

7.6 Trunking

Port Trunking, LACP Trunking

Port Trunking

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use static-channel-group command to create a static aggregator, or add a member port to an already-existing static aggregator.

Use the no static-channel-group command to detach the port from the static aggregator.

3. Command Syntax:

```
static-channel-group <1-8>
no static-channel-group
```

<1-8> Channel group number.

Maximum 8 ports in static-channel-group 1 to 6.

Maximum 4 ports in static-channel-group 7 and 8.

4. Example:

The following example adding the interface fe1 (port 1) to static-channel-group 1:

```
switch_a(config)#interface fe1
switch_a(config-if)#static-channel-group 1
switch_a(config-if)#
```

LACP Trunking

Static Channel Group:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use static-channel-group command to create a static aggregator, or add a member port to an already-existing static aggregator.

Use the no static-channel-group command to detach the port from the static aggregator.

3. Command Syntax:

static-channel-group <1-8>

no static-channel-group

<1-8> Channel group number.

Maximum 8 ports in static-channel-group 1 to 6.

Maximum 4 ports in static-channel-group 7 and 8.

4. Example:

The following example adding the interface fe1 (port 1) to static-channel-group 1:

```
switch_a(config)#interface fe1
switch_a(config-if)#static-channel-group 1
switch_a(config-if)#
```

Channel Group:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use channel-group command to add a port to a channel group specified by the channel group number (<1 3>). This command enables link aggregation on a port, so that it may be selected for aggregation by the local system.

Use the no channel-group command to turn off link aggregation on a port.

3. Command Syntax:

channel-group <1 | 3> mode MODE

no channel-group

<1 | 3> Channel group number.

1 Channel group number 1 for FE ports.

3 Channel group number 3 for GE ports.

Maximum 4 ports in channel-group 1.

Maximum 4 ports in channel-group 3.

MODE

active Enable initiation of LACP negotiation on a port.

passive Disable initiation of LACP negotiation on a port.

4. Example:

The following example enalbes initiation of LACP negotiation on the interface fe1 (port 1) to channel-group 1:

```
switch_a(config)#interface fe1
switch_a(config-if)#channel-group 1 mode active
switch_a(config-if)#
```

Clear LACP Counters:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use this command to clear all counters of all present LACP aggregators or a given LACP aggregator.

3. Command Syntax:

```
clear lacp (<1-65535>) counters
```

<1–65535> Channel-group number.

4. Example:

The following example clears all counters of LACP channel group 1:

```
switch_a#clear lacp 1 counters
switch_a#
```

LACP Port Priority:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use lacp port-priority command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the no lacp port-priority command to reset the priority of port to the default value (32768).

3. Command Syntax:

```
lacp port-priority <1-65535>
no lacp port-priority
```

<1–65535> Specify the LACP port priority.

4. Example:

The following example sets the LACP port priority 34 of interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lacp port-priority 34
switch_a(config-if)#
```

LACP Timeout:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use lacp timeout command to set the short or long timeout on a port. The default is long timeout

3. Command Syntax:

```
lacp timeout short | long
```

timeout Number of seconds before invalidating a received LACP data unit (DU).

short LACP short timeout. Short timeout value is 3 seconds.

long LACP long timeout. Long timeout value is 90 seconds.

4. Example:

The following example sets the LACP short timeout on interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lacp timeout short
switch_a(config-if)#
```

LACP System Priority:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use lacp system-priority command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups. Note: Lower numerical values have higher priorities.

Use no lacp system-priority command to reset the system priority of the local system to the default value (32768).

3. Command Syntax:

```
lacp system-priority <1-65535>
```

no lacp system-priority

<1-65535> LACP system priority. The default system priority is 32768.

4. Example:

The following example sets the LACP system priority 6700:

```
switch_a(config)#lacp system-priority 6700
switch_a(config)#
```

7.7 STP/Ring

Global Configuration, RSTP Port Setting, MSTP Properties, MSTP Instance Setting, MSTP Port Setting, Ring Setting, Chain Setting, Chain Pass-Through Setting, Advanced Setting

Global Configuration

STP Version:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to choose the Spanning Tree protocol, Rapid Spanning Tree protocol, or Multiple Spanning Tree protocol on a bridge.

3. Command Syntax:

bridge GROUP protocol PROTOCOL vlan-bridge

GROUP <1-1> Bridge group name used for bridging.

PROTOCOL

ieee IEEE 802.1Q spanning-tree protocol.

mstp IEEE 802.1s multiple spanning-tree protocol.

rstp IEEE 802.1w rapid spanning-tree protocol.

4. Example:

The following example chooses the PROTOCOL (rstp) on bridge GROUP (1):

```
switch_a(config)#bridge 1 protocol rstp vlan-bridge
switch_a(config)#
```

Multiple Spanning Tree Protocol:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to enable the Multiple Spanning Tree protocol on a bridge.

Use the no form of the command to disable the Multiple Spanning Tree protocol on a bridge.

3. Command Syntax:

```
bridge GROUP multiple-spanning-tree enable
no bridge GROUP multiple-spanning-tree enable BRIDGE-FORWARD
```

GROUP <1-1> Bridge group name used for bridging.

BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables or disables the multiple-spanning-tree on bridge GROUP (1):

```
switch_a(config)#bridge 1 multiple-spanning-tree enable
switch_a(config)#no bridge 1 multiple-spanning-tree enable bridge-forward
switch_a(config)#
```

Rapid Spanning Tree Protocol:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the Rapid Spanning Tree protocol on a bridge.

Use the no form of the command to disable the Rapid Spanning Tree protocol on a bridge.

3. Command Syntax:

```
bridge GROUP rapid-spanning-tree enable
no bridge GROUP rapid-spanning-tree enable BRIDGE-FORWARD
```

GROUP <1-1> Bridge group name used for bridging.

BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables or disables the rapid-spanning-tree on bridge GROUP (1):

```
switch_a(config)#bridge 1 rapid-spanning-tree enable
switch_a(config)#no bridge 1 rapid-spanning-tree enable bridge-forward
switch_a(config)#
```

Spanning Tree Protocol:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the Spanning Tree protocol on a bridge.

Use the no form of the command to disable the Spanning Tree protocol on a bridge.

3. Command Syntax:

```
bridge GROUP spanning-tree enable
no bridge GROUP spanning-tree enable BRIDGE-FORWARD
```

GROUP <1-1> Bridge group name used for bridging.

BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables or disables the spanning-tree on bridge GROUP (1):

```
switch_a(config)#bridge 1 spanning-tree enable
switch_a(config)#no bridge 1 spanning-tree enable bridge-forward
switch_a(config)#
```

Bridge Priority (0..61440):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root.

3. Command Syntax:

```
bridge GROUP priority PRIORITY
no bridge GROUP priority
```

GROUP <1-1> The ID of the bridge group for which the priority is set.

PRIORITY <0-61440> The bridge priority.

4. Example:

The following example sets the priority PRIORITY (4096) of bridge GROUP (1):

```
switch_a(config)#bridge 1 priority 4096
switch_a(config)#
```

Hello Time (sec) (1..9):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs).

3. Command Syntax:

```
bridge GROUP hello-time HELLOTIME
no bridge GROUP hello-time
```

GROUP <1-1> The ID of the bridge group to which this hello time is assigned.

HELLOTIME <1-9> The hello BPDU interval in seconds.

4. Example:

The following example sets the hello-time HELLOTIME (9) of bridge GROUP (1):

```
switch_a(config)#bridge 1 hello-time 9
switch_a(config)#
```

Max Age (sec) (6..28):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the max-age for a bridge.

Use the no parameter with this command to restore the default value of max-age.

3. Command Syntax:

```
bridge GROUP max-age MAXAGE
no bridge GROUP max-age
```

GROUP <1-1> The ID of the bridge group to which this maximum age time is assigned.

MAXAGE <6-28> The maximum time, in seconds, to listen for the root bridge.

4. Example:

The following example sets the max-age MAXAGE (28) of bridge GROUP (1):

```
switch_a(config)#bridge 1 max-age 28
switch_a(config)#
```

Forward Delay (sec) (4..30):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding.

Use the no parameter with this command to restore the default value.

3. Command Syntax:

```
bridge GROUP forward-time FORWARD_DELAY
no bridge GROUP forward-time
```

GROUP <1-1> The ID of the bridge group to which this delay time is assigned.

FORWARD_DELAY <4-30> the forwarding time delay in seconds.

4. Example:

The following example sets the forward-time FORWARD_DELAY (30) of bridge GROUP (1):

```
switch_a(config)#bridge 1 forward-time 30
switch_a(config)#
```

RSTP Port Setting

Priority(Granularity 16):

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the port priority for a bridge. The lower priority indicates a greater likelihood of the bridge becoming root.

3. Command Syntax:

```
bridge GROUP priority PRIORITY
```

GROUP <1-1> the ID of the bridge group.

PRIORITY <0-240> The priority to be assigned to the group.

4. Example:

The following example sets the priority PRIORITY (100) of the interface fe1 (port 1) of bridge GROUP (1):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge 1 priority 100
switch_a(config-if)#
```

Admin. Path Cost:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the cost of a path associated with a bridge-group.

Use the no parameter with this command to restore the default cost of a path associated with a bridge-group.

3. Command Syntax:

```
bridge GROUP path-cost PATHCOST
no bridge GROUP path-cost
```

GROUP <1-1> the ID of the bridge group.

PATHCOST <1-200000000> The cost to be assigned to the group.

4. Example:

The following example sets the cost (123) of the interface fe1 (port 1) of bridge GROUP (1):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge 1 path-cost 123
switch_a(config-if)#
```

Point to Point Link:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use spanning-tree link-type command to set the link type of a port to enable or disable rapid transition.

Use the no spanning-tree link-type command to set a port to its default state and to disable rapid transition.

3. Command Syntax:

```
(no) spanning-tree link-type LINKTYPE
```

LINKTYPE The link type to be assigned to the port.

point-to-point Enable rapid transition.

shared Disable rapid transition.

4. Example:

The following example sets the link-type LINKTYPE (point-to-point) of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree link-type point-to-point
switch_a(config-if)#
```

Autoedge:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use spanning-tree autoedge command to assist in automatic identification of the edge port.

Use the no spanning-tree autoedge command to disable this feature.

3. Command Syntax:

```
(no) spanning-tree autoedge
```

4. Example:

The following example enables the spanning-tree autoedge of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree autoedge
switch_a(config-if)#
```

Edgeport:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use spanning-tree edgeport command to set a port as an edge-port and to enable rapid transitions.

Use the no spanning-tree edgeport command to set a port to its default state (not an edge-port) and to disable rapid transitions.

3. Command Syntax:

```
(no) spanning-tree edgeport
```

4. Example:

The following example enables the spanning-tree edgeport of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree edgeport
switch_a(config-if)#
```

MSTP Properties

Region Name:

1. Command Mode: MST Configuration mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to MST Configuration mode.

The switch_a(config-mst)# prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:

Use this command to create an MST region and specify a name to it. MST bridges of a region form different spanning trees for different VLANs. By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

3. Command Syntax:

```
bridge GROUP region REGION_NAME
no bridge GROUP region
```

GROUP <1-1> Specify the bridge-group ID.

REGION_NAME Specify the name of the region.

4. Example:

The following example creates an MST region and specifies a name (regionname) to it in bridge GROUP (1):

```
Switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 region regionname
switch_a(config-mst)#
```

Revision Level:

1. Command Mode: MST Configuration mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to MST Configuration mode.

The switch_a(config-mst)# prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:

Use this command to specify the number for configuration information. The default value of revision number is 0.

3. Command Syntax:

```
bridge GROUP revision REVISION_NUM
```

GROUP <1-1> Specify the bridge-group ID.

REVISION_NUM <0-255> Revision number.

4. Example:

The following example specifies a revision number (25) of MST configuration in bridge GROUP (1):

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 revision 25
switch_a(config-mst)#
```

Max Hops:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the maximum allowed hops for BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the max hops for a BPDU prevents the messages from looping indefinetely in the network. When a bridge receives a MST BPDU that has exceeded the allowed max-hops, it discards the BPDU.

3. Command Syntax:

```
bridge GROUP max-hops HOP_COUNT
no bridge GROUP max-hops
```

GROUP <1-1> Specify the bridge-group ID.

HOP_COUNT Maximum hops the BPDU will be valid for.

4. Example:

The following example specifies the maximum allowed hops (25) for BPDU in bridge GROUP (1):

```
switch_a(config)#bridge 1 max-hops 25
switch_a(config)#
```

MSTP Instance Setting

Bridge Instance VLAN:

1. Command Mode: MST Configuration mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to MST Configuration mode.

The switch_a(config-mst)# prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge. This command can be used only after the VLANs are defined. Use the no parameter with this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

3. Command Syntax:

```
bridge GROUP instance INSTANCE_ID vlan VLAN_ID
no bridge GROUP instance INSTANCE_ID vlan VLAN_ID
```

GROUP <1-1> Specify the bridge-group ID.

INSTANCE_ID <1-15> Specify the instance ID.

VLAN_ID <1-4094> Specify multiple VLAN IDs corresponding to the bridge instance

4. Example:

The following example associates multiple VLANs (10) and (20) to instance (1) of bridge GROUP (1):

```
switch_a(config)#bridge 1 protocol mstp
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 instance 1 vlan 10, 20
switch_a(config-mst)#
```

Bridge Instance Priority:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default value of the bridge priority. The lower the priority of the bridge, the better the chances are the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096.

3. Command Syntax:

```
bridge GROUP instance INSTANCE_ID priority BRIDGE_PRIORITY
no bridge GROUP instance INSTANCE_ID priority
```

GROUP <1-1> Specify the bridge-group ID.

INSTANCE_ID Specify the instance ID.

BRIDGE_PRIORITY <0-61440> Specify the bridge priority.

4. Example:

The following example sets the bridge priority (0) for an MST instance (3) in bridge GROUP (1):

```
switch_a(config)#bridge 1 instance 3 priority 0
switch_a(config)#
```

MSTP Port Setting

Bridge-Group Instance:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to assign a Multiple Spanning Tree instance to a port. Use the no parameter with this command to remove the instance.

3. Command Syntax:

```
bridge GROUP instance INSTANCE_ID
no bridge GROUP instance INSTANCE_ID
```

GROUP <1-1> Specify the bridge-group ID.

INSTANCE_ID Specify the instance ID.

4. Example:

The following example assigns a Multiple Spanning Tree instance (3) to a port (fe1) in bridge GROUP (1):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3
switch_a(config-if)#
```

Bridge-Group Instance Priority:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the port priority for a bridge group. The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others. The permitted range is 0-240. The priority values can only be set in increments of 16.

3. Command Syntax:

```
bridge GROUP instance INSTANCE_ID priority PRIORITY
```

GROUP <1-1> Specify the bridge-group ID.

INSTANCE_ID <1-15> Specify the instance ID.

PRIORITY <0-240> Specify the port priority in a range of <0-240>.

4. Example:

The following example sets the port priority (121) for Multiple Spanning Tree instance (3) to a port (fe1) in bridge GROUP (1):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3 priority 121
switch_a(config-if)#
```

Bridge-Group Instance Path-Cost:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the cost of a path associated with an interface. Use the no parameter with this command to restore the default cost value of the path. A lower path-cost indicates a greater likelihood of the specific interface becoming a root.

3. Command Syntax:

```
bridge GROUP instance INSTANCE_ID path-cost PATH_COST
```

GROUP <1-1> Specify the bridge-group ID.

INSTANCE_ID <1-15> Specify the instance ID.

PATH_COST <1-200000000> Specify the cost of path in the range of <1-200000000>.

4. Example:

The following example sets the path cost (1000) for Multiple Spanning Tree instance (3) to a port (fe1) in bridge GROUP (1):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3 path-cost 1000
```

switch_a(config-if)#

Ring Setting

Ring state:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to enable Ring state. Use the no parameter with this command to disable Ring state.

3. Command Syntax:

bridge GROUP protocol ring

no bridge GROUP ring enable BRIDGE-FORWARD

GROUP <1-1> Specify the bridge-group ID.

BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables Ring state in bridge GROUP (1):

switch_a(config)#bridge 1 protocol ring

switch_a(config)#

Set ring port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set Ring port 1 and Ring port 2.

3. Command Syntax:

ring set-port RING_PORT_1 RING_PORT_2

RING_PORT_1 Specify the Ring port 1.

RING_PORT_2 Specify the Ring port 2.

4. Example:

The following example sets the fe1 and fe2 as Ring port 1 and Ring port 2:

switch_a(config)#ring set-port fe1 fe2

switch_a(config)#

Ring-coupling state:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to enable Ring-coupling state. Use the no parameter with this command to disable Ring-coupling state.

3. Command Syntax:

```
(no) ring-coupling enable
```

4. Example:

The following example enables Ring-coupling state:

```
switch_a(config)#ring-coupling enable
switch_a(config)#
```

Set ring-coupling port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set Ring-coupling port 1 and Ring-coupling port 2.

3. Command Syntax:

```
ring set-coupling-port COUPLING_PORT_1 COUPLING_PORT_2
```

COUPLING_PORT_1 Specify the Ring-coupling port 1.

COUPLING_PORT_2 Specify the Ring-coupling port 2.

4. Example:

The following example sets the fe3 and fe4 as Ring-coupling port 1 and Ring-coupling port 2:

```
switch_a(config)#ring set-coupling-port fe3 fe4
switch_a(config)#
```

Chain Setting

Chain Protocol:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set Chain Protocol to an interface. Use the no parameter with this command to revoke Chain Protocol from an interface.

3. Command Syntax:

chain port enable

no chain port

4. Example:

The following example sets Chain Protocol to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#chain port enable
switch_a(config-if)#
```

VLAN:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the Switch priority for running chain protocol. Switch with lower priority will run as Master (forwarding) port. Use the no form of the command to restore default value (1).

3. Command Syntax:

bridge <1-1> chain-vlan <1-4094>

no bridge <1-1> chain-vlan

<1–1> Bridge Group name for bridging.

<1–4094> The VID of the VLAN for chain on the bridge <1-4094>.

4. Example:

The following example sets VLAN ID (1) for chain on bridge GROUP (1):

```
switch_a(config)#bridge 1 chain-vlan 1
switch_a(config)#
```

Chain Priority:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the Switch priority for running chain protocol. Switch with lower priority will run as Master (forwarding) port. Use the no form of the command to restore default value (128).

3. Command Syntax:

```
bridge GROUP chain-priority <0-255>
no bridge GROUP chain-priority
```

Group = <1-1> Bridge Group name for bridging.

<0-255> The Switch priority for running chain protocol.

4. Example:

The following example sets the new Switch priority (10) to bridge GROUP (1):

```
switch_a(config)#bridge 1 chain-priority 10
switch_a(config)#
```

Chain Timeout:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the Switch timeout count for running chain protocol. Chain recovery time = (Chain Timeout Count – 1) x 200ms.

Use the no form of the command to restore default value (5).

Default Chain recovery time = (5 – 1) x 200ms = 800ms.

3. Command Syntax:

```
bridge GROUP chain-timeout <3-255>
no bridge GROUP chain-timeout
```

Group = <1-1> Bridge Group name for bridging.

<3-255> The Switch timeout count for running chain protocol.

4. Example:

The following example sets the new Switch timeout (10) to bridge GROUP (1):

```
switch_a(config)#bridge 1 chain-timeout 10
switch_a(config)#
```

Storm Control:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable Storm Control (broadcast and multicast) for Chain Protocol setting. Use the no form of the command to disable Storm Control (broadcast and multicast) for Chain Protocol setting.

3. Command Syntax:

```
bridge GROUP chain-storm enable
no bridge GROUP chain-storm
```

Group = <1-1> Bridge Group name for bridging.

4. Example:

The following example enables chain storm control for bridge GROUP (1):

```
switch_a(config)#bridge 1 chain-storm enable
switch_a(config)#
```

Chain Pass-Through Setting

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set chain pass-through port 1 and chain pass-through port 2.

3. Command Syntax:

```
chain pass-through IFNAME IFNAME
no chain pass-through
```

IFNAME Chain pass-through port number 1.

IFNAME Chain pass-through port number 2.

4. Example:

The following example enables the fe3 and fe4 as chain pass-through port 1 and chain pass-through port 2:

```
switch_a(config)#chain pass-through fe3 fe4
switch_a(config)#
```

Advanced Setting

Advanced Bridge Configuration:

Bridge bpdu-guard configuration:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge.

Use the no parameter with this command to disable the BPDU Guard feature on a bridge.

When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have bpdu-guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.

3. Command Syntax:

```
bridge GROUP spanning-tree portfast bpdu-guard
no bridge GROUP spanning-tree portfast bpdu-guard
```

GROUP <1-1> Bridge-group ID used for bridging.

4. Example:

The following example enables the BPDU Guard feature on bridge GROUP (1):

```
switch_a(config)#bridge 1 spanning-tree portfast bpdu-guard
switch_a(config)#
```

Error disable timeout configuration:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the timeout mechanism for the port to be enabled back for a bridge.

Use the no parameter with this command to disable the timeout mechanism for the port to be enabled back for a bridge.

3. Command Syntax:

```
bridge GROUP spanning-tree errdisable-timeout enable
no bridge GROUP spanning-tree errdisable-timeout enable
```

GROUP <1-1> Bridge-group ID used for bridging.

4. Example:

The following example enables the timeout mechanism for the port to be enabled back for bridge GROUP (1):

```
switch_a(config)#bridge 1 spanning-tree errdisable-timeout enable
switch_a(config)#
```

Interval:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the time interval after which a port is brought back up. The range of interval value is from 10 to 1000000. And the default value is 300 seconds.

3. Command Syntax:

bridge GROUP spanning-tree errdisable-timeout interval <10-1000000>

no bridge GROUP spanning-tree errdisable-timeout interval

GROUP <1-1> Bridge-group ID used for bridging.

<10-1000000> The error disable timeout interval in seconds.

4. Example:

The following example sets error disable timeout interval time 100 seconds for bridge GROUP (1):

```
switch_a(config)#bridge 1 spanning-tree errdisable-timeout interval 100
switch_a(config)#
```

Advanced Per Port Configuration:

Portfast configuration / status:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

3. Command Syntax:

spanning-tree portfast

no spanning-tree portfast

4. Example:

The following example sets the interface fe1 (port 1) as an edge-port and to enable rapid transitions:

```
switch_a(config)#interface fe1
switch_a(config-if)# spanning-tree portfast
switch_a(config-if)#
```

Bpdu-guard configuration:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enable or disable the BPDU Guard feature on a port.

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

This command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge level BPDU-Guard configuration takes effect.

3. Command Syntax:

```
spanning-tree portfast bpdu-guard (enable disable default)
no spanning-tree portfast bpdu-guard
```

4. Example:

The following example enables the BPDU Guard feature on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)# spanning-tree portfast bpdu-guard enable
switch_a(config-if)#
```

7.8 VLAN

VLAN Mode Setting, 802.1Q VLAN Setting, 802.1Q Port Setting, Port Based VLAN

802.1Q VLAN Setting

VLAN Database:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use vlan database command to enter the VLAN configuration mode.

3. Command Syntax:

```
vlan database
```

4. Example:

The following example changes to VLAN configuration mode from Configure mode:

```
switch_a(config)#vlan database
switch_a(config-vlan)#
```

Add VLAN/Delete VLAN:

1. Command Mode: VLAN Configure mode

Logon to Configure Mode (Configure Terminal Mode).

Logon to VLAN Configure Mode.

The switch_a(config-vlan)# prompt will show on the screen.

```
switch_a(config)#vlan database
switch_a(config-vlan)#
```

2. Usage:

This command enables or disables the state of a particular VLAN on a bridge basis. Specifying the disable state causes all forwarding over the specified VLAN ID on the specified bridge to cease. Specifying the enable state allows forwarding of frames on the specified VLAN-aware bridge.

3. Command Syntax:

```
vlan VLANID bridge GROUP name VLAN_NAME state enable/disable
no vlan VLANID bridge GROUP
```

VLANID The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.

GROUP <1-1> The ID of the bridge-group on which the VLAN will be affected.

VLAN_NAME The ASCII name of the VLAN. Maximum length: 16 characters.

enable Sets VLAN into an enable state.

disable Sets VLAN into a disable state.

4. Example:

The following example enables the vlan VLANID (2) and name VLAN_NAME (vlan2) of bridge GROUP (1):

```
switch_a(config-vlan)#vlan 2 bridge 1 name vlan2 state enable
switch_a(config-vlan)#
```

802.1Q Port Setting

Switchport mode access:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use switchport mode access command to set the switching characteristics of the Layer-2 interface to access mode, and classify untagged frames only.

Use the no switchport access command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:

```
switchport mode access
no switchport access
```

4. Example:

The following example sets the switchport mode access of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode access
switch_a(config-if)#
```

Switchport mode hybrid:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use switchport mode hybrid command to set the switching characteristics of the Layer-2 interface as hybrid, and classify both tagged and untagged frames.

Use the no switchport hybrid command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:

```
switchport mode hybrid
switchport mode hybrid acceptable-frame-type all/vlan-tagged
no switchport hybrid
```

all Set all frames can be received.

vlan-tagged Set vlan-tagged frames can only be received.

4. Example:

The following example sets the switchport mode hybrid of the interface fe1 (port 1) and all frames to be received on interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode hybrid acceptable-frame-type all
switch_a(config-if)#
```

Switchport mode trunk:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use switchport mode trunk command to set the switching characteristics of the Layer-2 interface as trunk, and specify only tagged frames.

Use the no switchport trunk command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:

```
switchport mode trunk
no switchport trunk
```

4. Example:

The following example sets the switchport mode trunk of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode trunk
switch_a(config-if)#
```

Switchport hybrid allowed vlan:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the switching characteristics of the Layer-2 interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Use the no parameter to turn off allowed hybrid switching.

3. Command Syntax:

```
switchport hybrid allowed vlan all
switchport hybrid allowed vlan none
switchport hybrid allowed vlan add VLANID egress-tagged enable/disable
```

switchport hybrid allowed vlan remove VLANID

no switchport hybrid vlan

all Allow all VLANs to transmit and receive through the Layer-2 interface.

none Allow no VLANs to transmit and receive through the Layer-2 interface.

add Add a VLAN to the member set.

remove Remove a VLAN from the member set.

VLANID <2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer-2 interface.

For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.

For a VLAN list, specify the VLAN numbers separated by commas.

egress-tagged

enable Enable the egress tagging for the outgoing frames.

disable Disable the egress tagging for the outgoing frames.

4. Example:

The following example specifies to add the interface fe1 (port 1) to VLANID (2) and enable the egress-tagged for the outgoing frames on interface fe1 (port 1):

switch_a(config)#interface fe1

switch_a(config-if)#switchport hybrid allowed vlan add 2 egress-tagged enable

switch_a(config-if)#

Switchport trunk allowed vlan:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

switch_a(config)#interface fe1

switch_a(config-if)#

2. Usage:

Use this command to set the switching characteristics of the Layer-2 interface to trunk. The all parameter indicates that any VLAN ID is part of its port's member set. The none parameter indicates that no VLAN ID is configured on this port. The add and remove parameters will add and remove VLAN IDs to/from the port's member set.

Use the no parameter to remove all VLAN IDs configured on this port.

3. Command Syntax:

switchport trunk allowed vlan all

switchport trunk allowed vlan none

switchport trunk allowed vlan add VLANID

switchport trunk allowed vlan remove VLANID

```
switchport trunk allowed vlan except VLANID
no switchport trunk vlan
```

all Allow all VLANs to transmit and receive through the Layer-2 interface.

none Allow no VLANs to transmit and receive through the Layer-2 interface.

add Add a VLAN to transmit and receive through the Layer-2 interface.

remove Remove a VLAN from transmit and receive through the Layer-2 interface.

except All VLANs, except the VLAN for which the ID is specified, are part of its ports member set.

VLANID <2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer-2 interface. A single VLAN, VLAN range, or VLAN list can be set.

For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.

For a VLAN list, specify the VLAN numbers separated by commas.

4. Example:

The following example specifies to add the interface fe1 (port 1) to VLANID (2):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport trunk allowed vlan add 2
switch_a(config-if)#
```

Priority Level:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set user priority for port.

3. Command Syntax:

```
user-priority <0-7>
```

<0-7> User priority value.

4. Example:

The following example sets user priority (0) for the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#user-priority 0
switch_a(config-if)#
```

Port Based VLAN

Switchport portbase add/remove vlan:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set or remove the default VLAN for the interface.

3. Command Syntax:

```
switchport portbase add remove vlan VLANID
```

VLANID The ID of the VLAN will be added to or removed from the Layer-2 interface.

4. Example:

The following example specifies to add the interface fe1 (port 1) to VLANID (2):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport portbase add vlan 2
switch_a(config-if)#
```

7.9 QoS

Global Configuration, 802.1p Priority, DSCP

Global Configuration

QoS:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use mls qos enable command to globally enable QoS.

Use the no mls qos command to globally disable QoS.

3. Command Syntax:

```
mls qos enable
(no) mls qos
```

4. Example:

The following example globally enables QoS on the switch:

```
switch_a(config)#mls qos enable
switch_a(config)#
```

Trust:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use mls qos trust command to turn on QoS trust CoS or DSCP.

Use the no mls qos trust command to turn off QoS trust CoS or DSCP.

3. Command Syntax:

```
(no) mls qos trust cos/dscp
```

cos Class of Service.

dscp Differentiated Service Code Point.

4. Example:

The following example turns on QoS trust CoS on the switch:

```
switch_a(config)#mls qos trust cos
switch_a(config)#
```

Strict Priority:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use priority-queue out command to enable the egress expedite queue.

Use the no priority-queue out command to disable the egress expedite queue.

3. Command Syntax:

```
(no) priority-queue out
```

4. Example:

The following example enables the egress expedite queue on the switch:

```
switch_a(config)#priority-queue out
switch_a(config)#
```

Weighted Round Robin:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use wrr-queue bandwidth command to specify the bandwidth ratios of the transmit queues.

3. Command Syntax:

```
wrr-queue bandwidth WRR_WTS
```

WRR_WTS Weighted Round Robin (WRR) weights for the 4 queues (4 values separated by spaces). Range is 1-55.

4. Example:

The following example specifies the bandwidth ratios of the transmit queues on the switch:

```
switch_a(config)#wrr-queue bandwidth 1 2 4 8
switch_a(config)#
```

802.1p Priority

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use wrr-queue cos-map command to specify CoS values for a queue.

3. Command Syntax:

```
wrr-queue cos-map QUEUE_ID COS_VALUE
```

QUEUE_ID Queue ID. Range is 0-3.

COS_VALUE CoS values. Up to 8 values (separated by spaces). Range is 0-7.

4. Example:

The following example shows mapping CoS values 0 and 1 to queue 1 on the switch:

```
switch_a(config)#wrr-queue cos-map 1 0 1
switch_a(config)#
```

DSCP

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use mls qos map dscp-queue command to map the DSCP values to a queue.

3. Command Syntax:

mls qos map dscp-queue DSCP_VALUE to QUEUE_ID

DSCP_VALUE DSCP values. Up to 8 values (separated by spaces). Range is 0-63.

QUEUE_ID Queue ID. Range is 0-3.

4. Example:

The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

```
switch_a(config)#mls qos map dscp-queue 0 1 2 3 to 1
switch_a(config)#
```

7.10 SNMP

SNMP General Setting, SNMP v1/v2c, SNMP v3

SNMP General Setting

SNMP Status:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server enable command to enable and no snmp-server enable command to disable SNMP to the switch.

3. Command Syntax:

(no) snmp-server enable

4. Example:

The following example enables SNMP to the switch:

```
switch_a(config)#snmp-server enable
switch_a(config)#
```

Description:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server description command to specify and no snmp-server description command to remove description for SNMP.

3. Command Syntax:

snmp-server description DESCRIPTION

no snmp-server description

DESCRIPTION The description for SNMP.

4. Example:

The following example specifies description (description) for SNMP:

```
switch_a(config)#snmp-server description description
switch_a(config)#
```

Location:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server location command to specify and no snmp-server location command to remove location for SNMP.

3. Command Syntax:

```
snmp-server location LOCATION
no snmp-server location
```

LOCATION The location for SNMP.

4. Example:

The following example specifies location (location) for SNMP:

```
switch_a(config)#snmp-server location location
switch_a(config)#
```

Contact:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server contact command to specify and no snmp-server contact command to remove contact for SNMP.

3. Command Syntax:

```
snmp-server contact CONTACT
no snmp-server contact
```

CONTACT The contact for SNMP.

4. Example:

The following example specifies contact (contact) for SNMP:

```
switch_a(config)#snmp-server contact contact
```

switch_a(config)#

Trap Community Name:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to specify trap community name for SNMP.

Use the no parameter with this command to remove trap community name for SNMP.

3. Command Syntax:

snmp-server trap-community <1-5> NAME

no snmp-server trap-community <1-5>

<1-5> The trap community 1-5.

NAME The trap community name for SNMP.

4. Example:

The following example specifies trap community name 1 (name) for SNMP:

```
switch_a(config)#snmp-server trap-community 1 name
switch_a(config)#
```

Trap Host IP Address:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify trap host IP address for SNMP.

Use the no parameter with this command to remove trap host IP address for SNMP.

3. Command Syntax:

```
snmp-server trap-ipaddress <1–5> IP-ADDRESS
no snmp-server trap-ipaddress <1–5>
```

<1–5> The trap host IP address 1–5.

IP-ADDRESS The trap host IP address for SNMP. A.B.C.D specifies the IP address.

4. Example:

The following example specifies trap host 1 IP address (192.168.1.20) for SNMP:

```
switch_a(config)#snmp-server trap-ipaddress 1 192.168.1.20
switch_a(config)#
```

Link Down Trap:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server trap-type enable linkDown command to enable link down trap for SNMP.

Use the no snmp-server trap-type enable linkDown command to disable link down trap for SNMP.

3. Command Syntax:

```
(no) snmp-server trap-type enable linkDown
```

4. Example:

The following example enables link down trap for SNMP:

```
switch_a(config)#snmp-server trap-type enable linkDown
switch_a(config)#
```

Link Up Trap:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server trap-type enable linkUp command to enable link up trap for SNMP.

Use the no snmp-server trap-type enable linkUp command to disable link up trap for SNMP.

3. Command Syntax:

```
(no) snmp-server trap-type enable linkUp
```

4. Example:

The following example enables link up trap for SNMP:

```
switch_a(config)#snmp-server trap-type enable linkUp
switch_a(config)#
```

MAC Notification Trap:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the Switch to send MAC Notification Trap to the network management system (NMS).

Use the no parameter with this command to disable the Switch to send MAC Notification Trap to the network management system (NMS).

3. Command Syntax:

```
snmp-server trap-type enable mac-notification
no snmp-server trap-type enable mac-notification
```

4. Example:

The following example enables the Switch to send MAC Notification Trap to the network management system (NMS):

```
switch_a(config)#snmp-server trap-type enable mac-notification
switch_a(config)#
```

MAC Notification Interval:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the MAC notification trap interval in seconds between each set of traps that are generated.

3. Command Syntax:

```
snmp-server mac-notification interval <1–65535>
```

<1–65535> The MAC notification trap interval in seconds.

4. Example:

The following example sets MAC notification trap interval time 10 seconds:

```
switch_a(config)# snmp-server mac-notification interval 10
switch_a(config)#
```

MAC Notification History Size:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the maximum number of entries in the MAC notification history table.

3. Command Syntax:

```
snmp-server mac-notification history-size <1–500>
```

<1–500> The range is 1 to 500.

4. Example:

The following example sets the maximum 500 entries in the MAC notification history table:

```
switch_a(config)# snmp-server mac-notification history-size 500
switch_a(config)#
```

MAC Notification Added/Removed:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to add or remove MAC Notification Trap on an interface port.

3. Command Syntax:

```
snmp-server trap mac-notification (added | removed)
no snmp-server trap mac-notification (added | removed)
```

4. Example:

The following example specifies to add MAC Notification Trap on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)# snmp-server trap mac-notification added
switch_a(config-if)#
```

SNMP v1/v2c

Get Community Name:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server community get command to specify and no snmp-server community get command to remove get community name for SNMP.

3. Command Syntax:

```
snmp-server community get NAME
no snmp-server community get
```

NAME The get community name for SNMP.

4. Example:

The following example specifies get community name (name) for SNMP:

```
switch_a(config)#snmp-server community get name
switch_a(config)#
```

Set Community Name:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use snmp-server community set command to specify and no snmp-server community set command to remove set community name for SNMP.

3. Command Syntax:

```
snmp-server community set NAME
no snmp-server community set
```

NAME The set community name for SNMP.

4. Example:

The following example specifies set community name (name) for SNMP:

```
switch_a(config)#snmp-server community set name
switch_a(config)#
```

SNMP v3

SNMPv3 No-Auth:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Add a user using snmp v3 with read-only or read-write access mode and without authentication. Use the no form of the command to delete this user.

3. Command Syntax:

```
(no) snmp-server v3-user USERNAME (ro rw) noauth
```

USERNAME Specify a user name.

ro read-only access mode

rw read-write access mode

4. Example:

The following example adds a user (myuser) using snmp v3 with read-only access mode and without authentication:

```
switch_a(config)#snmp-server v3-user myuser ro noauth
switch_a(config)#
```

SNMPv3 Auth-MD5, SNMPv3 Auth-SHA:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Add a user using snmp v3 with read-only or read-write access mode and with MD5 or SHA authentication. Use the no form of the command to delete this user.

3. Command Syntax:

```
(no) snmp-server v3-user USERNAME (ro rw) auth (md5 sha) AUTH_PASSWORD
```

USERNAME Specify a user name.

ro read-only access mode

rw read-write access mode

md5 authentication method

sha authentication method

AUTH_PASSWORD authentication password

4. Example:

The following example adds a user (myuser) using snmp v3 with read-write access mode and MD5 authentication (mypassword):

```
switch_a(config)#snmp-server v3-user myuser rw auth md5 mypassword
switch_a(config)#
```

SNMPv3 Priv Auth-MD5, SNMPv3 Priv Auth-SHA:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Add a user using snmp v3 with read-only or read-write access mode, MD5 or SHA authentication, and privacy. Use the no form of the command to delete this user.

3. Command Syntax:

```
(no) snmp-server v3-user USERNAME (ro rw) priv auth (md5 sha) AUTH_PASSWORD des PRIV_PASS_PHRASE
```

USERNAME Specify a user name.

ro read-only access mode

rw read-write access mode

md5 authentication method

sha authentication method

AUTH_PASSWORD authentication password

PRIV_PASS_PHRASE encryption pass phrase

4. Example:

The following example adds a user (myuser) using snmp v3 with read-write access mode, MD5 authentication (mypassword), and encryption pass phrase (mypassphrase):

```
switch_a(config)#snmp-server v3-user myuser rw priv md5 mypassword des mypassphrase
switch_a(config)#
```

7.11 802.1x

Radius Configuration, Port Authentication

Radius Configuration

Radius Status:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use dot1x system-auth-ctrl command to globally enable authentication.

Use no dot1x system-auth-ctrl command to globally disable authentication.

3. Command Syntax:

```
(no) dot1x system-auth-ctrl
```

4. Example:

The following example globally enables authentication:

```
switch_a(config)#dot1x system-auth-ctrl
switch_a(config)#
```

Radius Server IP:

Radius Server Port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the IP address of the remote radius server host and assign authentication and accounting destination port number.

3. Command Syntax:

```
(no) radius-server host IP-ADDRESS auth-port PORT
```

IP-ADDRESS A.B.C.D specifies the IP address of the radius server host.

PORT specifies the UDP destination port for authentication requests. The host is not used for authentication if set to 0.

4. Example:

The following example specifies the IP address (192.168.1.100) of the remote radius server host and assigns authentication and accounting destination port number (1812):

```
switch_a(config)#radius-server host 192.168.1.100 auth-port 1812
switch_a(config)#
```

Secret Key:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the shared secret key between a Radius server and a client.

3. Command Syntax:

```
(no) radius-server host IP-ADDRESS key KEY
```

IP-ADDRESS A.B.C.D specifies the IP address of the radius server host.

KEY specifies the secret key shared among the radius server and the 802.1x client.

4. Example:

The following example specifies the IP address (192.168.1.100) of the remote radius server host and set the secret key (ipi) shared among the radius server and the 802.1x client:

```
switch_a(config)#radius-server host 192.168.1.100 key ipi
switch_a(config)#
```

Timeout:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the number of seconds a Switch waits for a reply to a radius request before retransmitting the request.

3. Command Syntax:

```
radius-server timeout SEC
no radius-server timeout
```

SEC <1–1000> The number of seconds for a Switch to wait for a server host to reply before timing out. Enter a value in the range 1 to 1000.

4. Example:

The following example specifies 20 seconds for the Switch to wait for a server host to reply before timing out:

```
switch_a(config)#radius-server timeout 20
switch_a(config)#
```

Retransmit:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the number of times the Switch transmits each radius request to the server before giving up.

3. Command Syntax:

```
radius-server retransmit RETRIES
no radius-server retransmit
```

RETRIES <1-100> Specifies the retransmit value. Enter a value in the range 1 to 100.

4. Example:

The following example specifies the retransmit value 12:

```
switch_a(config)#radius-server retransmit 12
switch_a(config)#
```

Port Authentication

Authentication State:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use dot1x reauthetication command to enable reauthentication on a port.

Use no dot1x reauthetication command to disable reauthentication on a port.

3. Command Syntax:

```
(no) dot1x reauthentication
```

4. Example:

The following example specifies to enable reauthetication on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x reauthentication
switch_a(config-if)#
```

Port Control:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to force a port state.

Use no dot1x port-control command to remove a port from the 802.1x management.

3. Command Syntax:

```
dot1x port-control auto force-authorized force-unauthorized
no dot1x port-control
```

auto Specify to enable authentication on port.

force-authorized Specify to force a port to always be in an authorized state.

force-unauthorized Specify to force a port to always be in an unauthorized state.

4. Example:

The following example specifies to enable authetication on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x port-control auto
switch_a(config-if)#
```

Periodic Reauthentication:

Reauthentication Period:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set the interval between reauthorization attempts.

Use no dot1x timeout re-authperiod command to delete the interval between reauthorization attempts.

3. Command Syntax:

```
dot1x timeout re-authperiod SECS
no dot1x timeout re-authperiod
```

SECS <1-4294967295> Specify the seconds between reauthorization attempts. The default time is 3600 seconds.

4. Example:

The following example specifies to set the interval 25 seconds between reauthorization attempts:

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x timeout re-authperiod 25
switch_a(config-if)#
```

7.12 LLDP

LLDP General Settings, LLDP Ports Settings, LLDP Neighbors, LLDP Statistics

LLDP General Setting

LLDP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable Link Layer Discovery Protocol (LLDP) globally.

Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) globally.

3. Command Syntax:

```
(no) lldp enable
```

4. Example:

The following example enables Link Layer Discovery Protocol (LLDP) globally:

```
switch_a(config)#lldp enable
switch_a(config)#
```

Holdtime Multiplier (2–10):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the Link Layer Discovery Protocol (LLDP) holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) that the switch advertises to the neighbors.

3. Command Syntax:

```
lldp holdtime multiplier <2-10>
```

<2–10> Holdtime multiplier 2-10, default is 4.

4. Example:

The following example sets Link Layer Discovery Protocol (LLDP) holdtime multiplier to 5:

```
switch_a(config)#lldp holdtime multiplier 5
switch_a(config)#
```

Tx Interval (5-32768 seconds):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set the transmit interval. This is the interval between regular transmissions of Link Layer Discovery Protocol (LLDP) advertisements.

3. Command Syntax:

lldp txinterval <5–32768>

<5–32768> TxInterval 5-32768 seconds, default is 30 seconds.

4. Example:

The following example sets Link Layer Discovery Protocol (LLDP) transmit interval to 60 seconds:

```
switch_a(config)#lldp txinterval 60
switch_a(config)#
```

Global TLV Setting:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to configure Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.

Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.

3. Command Syntax:

(no) lldp tlv-global port-descr | sys-name | sys-descr | sys-cap | mgmt-addrs | port-vlan-id | mac-phy | protocol-identity | vlan-name | port-and-protocol | power-mdi | link-aggregation | max-frame

port-descr Port Description TLV.

sys-name System Name TLV.

sys-descr System Description TLV.

sys-cap System Capabilities TLV.

mgmt-addrs Management Address TLV.

port-vlan-id Port VLAN ID TLV.

mac-phy MAC/PHY Configuration/Status TLV.

protocol-identity Protocol Identity TLV.

vlan-name VLAN Name TLV.

port-and-protocol Port And Protocol VLAN ID TLV.

power-mdi Power Via MDI TLV.

link-aggregation Link Aggregation TLV.

max-frame Maximum Frame Size TLV.

4. Example:

The following example sets Link Layer Discovery Protocol (LLDP) Link Aggregation Type Length Value (TLV):

```
switch_a(config)#lldp tlv-global link-aggregation
switch_a(config)#
```

LLDP Ports Settings

Transmit:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to send Link Layer Discovery Protocol (LLDP) packets on the interface.

Use the no parameter with this command to disallow sending Link Layer Discovery Protocol (LLDP) packets on the interface.

3. Command Syntax:

```
(no) lldp tx-pkt
```

4. Example:

The following example sends Link Layer Discovery Protocol (LLDP) packets on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp tx-pkt
switch_a(config-if)#
```

Receive:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to receive Link Layer Discovery Protocol (LLDP) packets on the interface.

Use the no parameter with this command to disallow receiving Link Layer Discovery Protocol (LLDP) packets on the interface.

3. Command Syntax:

(no) lldp rcv-pkt

4. Example:

The following example receives Link Layer Discovery Protocol (LLDP) packets on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp rcv-pkt
switch_a(config-if)#
```

Notify:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enable Link Layer Discovery Protocol (LLDP) notification on the interface.

Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) notification on the interface.

3. Command Syntax:

(no) lldp notification

4. Example:

The following example enables Link Layer Discovery Protocol (LLDP) notification on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp notification
switch_a(config-if)#
```

TLVs:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

fe1 means port 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to configure Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.

Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.

3. Command Syntax:

```
(no) lldp tlv-global port-descr | sys-name | sys-descr | sys-cap | mgmt-addrs | port-vlan-id | mac-phy | protocol-identity | vlan-name | port-and-protocol | power-mdi | link-aggregation | max-frame
```

port-descr Port Description TLV.

sys-name System Name TLV.

sys-descr System Description TLV.

sys-cap System Capabilities TLV.

mgmt-addrs Management Address TLV.

port-vlan-id Port VLAN ID TLV.

mac-phy MAC/PHY Configuration/Status TLV.

protocol-identity Protocol Identity TLV.

vlan-name VLAN Name TLV.

port-and-protocol Port And Protocol VLAN ID TLV.

power-mdi Power Via MDI TLV.

link-aggregation Link Aggregation TLV.

max-frame Maximum Frame Size TLV.

4. Example:

The following example sets Link Layer Discovery Protocol (LLDP) Link Aggregation Type Length Value (TLV) on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp tlv-global link-aggregation
switch_a(config-if)#
```

LLDP Neighbors

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use the show lldp neighbors command to show Link Layer Discovery Protocol (LLDP) neighbors information.

3. Command Syntax:

show lldp neighbors

4. Example:

The following example shows Link Layer Discovery Protocol (LLDP) neighbors information:

switch_a> show lldp neighbors

LLDP Statistics

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

switch_a>

switch_a#

2. Usage:

Use this command to show Link Layer Discovery Protocol (LLDP) statistics.

3. Command Syntax:

show lldp statistics

show lldp statistics IFNAME

IFNAME Interface name.

4. Example:

The following example shows Link Layer Discovery Protocol (LLDP) statistics:

switch_a> show lldp statistics

7.13 Other Protocols

GVRP, IGMP Snooping, NTP, GMRP, DHCP Server

GVRP

GVRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use set gvrp enable bridge command to enable (set) and set gvrp disable bridge command to disable (reset) GVRP globally for the bridge instance. This command does not enable/disable GVRP in all ports of the bridge. After enabling GVRP globally, use the set port gvrp enable command to enable GVRP on individual ports of the bridge.

3. Command Syntax:

set gvrp enable bridge GROUP

```
set gvrp disable bridge GROUP
```

GROUP Bridge-group ID used for bridging.

4. Example:

The following example globally enables GVRP to bridge GROUP (1):

```
switch_a(config)#set gvrp enable bridge 1
switch_a(config)#
```

Dynamic VLAN creation:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use set gvrp dynamic-vlan-creation enable bridge command to enable and set gvrp dynamic-vlan-creation disable bridge command to disable dynamic VLAN creation for a specific bridge instance.

3. Command Syntax:

```
set gvrp dynamic-vlan-creation enable bridge GROUP
set gvrp dynamic-vlan-creation disable bridge GROUP
```

GROUP Bridge-group ID used for bridging.

4. Example:

The following example enables dynamic VLAN creation for bridge GROUP (1):

```
switch_a(config)#set gvrp dynamic-vlan-creation enable bridge 1
switch_a(config)#
```

Per port setting:

GVRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use set port gvrp enable command to enable and set port gvrp disable command to disable GVRP on a port or all ports in a bridge.

3. Command Syntax:

```
set port gvrp enable all/IFNAME
set port gvrp disable all/IFNAME
```

all All ports added to recently configured bridge.

IFNAME The name of the interface.

4. Example:

The following example enables GVRP on the interface fe1 (port 1):

```
switch_a(config)#set port gvrp enable fe1
switch_a(config)#
```

Per port setting:

GVRP applicant:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set the GVRP applicant state to normal or active.

3. Command Syntax:

set gvrp applicant state active/normal IFNAME

active Active state

normal Normal state

IFNAME Name of the interface.

4. Example:

The following example sets GVRP applicant state to active on the interface fe1 (port 1):

```
switch_a(config)#set gvrp applicant state active fe1
switch_a(config)#
```

Per port setting:

GVRP registration:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to set GVRP registration to normal, fixed, and forbidden registration mode for a given port.

3. Command Syntax:

set gvrp registration normal IF_NAME

set gvrp registration fixed IF_NAME

set gvrp registration forbidden IF_NAME

normal Specify dynamic GVRP multicast registration and deregistration on the port.

fixed Specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.

forbidden Specify that all GVRP multicasts are deregistered, and prevent any further GVRP multicast registration on the port.

IF_NAME The name of the interface.

4. Example:

The following example sets GVRP registration to fixed registration mode on the interface fe1 (port 1):

```
switch_a(config)#set gvrp registration fixed fe1
switch_a(config)#
```

IGMP Snooping

IGMP mode:

Querier:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use ip igmp snooping querier command to enable IGMP querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

Use the no ip igmp snooping querier command to disable IGMP querier configuration.

3. Command Syntax:

(no) ip igmp snooping querier

4. Example:

The following example enables IGMP snooping querier:

```
switch_a(config)# ip igmp snooping querier
switch_a(config)#
```

IGMP mode:

Passive:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use ip igmp snooping command to enable IGMP Snooping. This command is given in the Global Config mode. IGMP Snooping is enabled at the switch level.

Use the no ip igmp snooping command to globally disable IGMP Snooping.

3. Command Syntax:

(no) ip igmp snooping enable

4. Example:

The following example enables IGMP snooping on the switch:

```
switch_a(config)# ip igmp snooping enable
switch_a(config)#
```

IGMP version:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp version command to set the current IGMP protocol version on an interface.

To return to the default version, use the no ip igmp version command.

3. Command Syntax:

ip igmp version VERSION

no ip igmp version

VERSION IGMP protocol version number.

4. Example:

The following example sets the IGMP protocol version 3 on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 3
switch_a(config-if)#
```

Fast-leave:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp snooping fast-leave command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate leave processing; the IGMP group-membership is removed, as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the no ip igmp snooping fast-leave command to disable fast-leave processing.

3. Command Syntax:

```
(no) ip igmp snooping fast-leave
```

4. Example:

The following example enables IGMP snooping fast-leave on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping fast-leave
switch_a(config-if)#
```

IGMP querier:

Query-interval:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp query-interval command to configure the frequency of sending IGMP host query messages.

To return to the default frequency, use the no ip igmp query-interval command.

3. Command Syntax:

```
ip igmp query-interval INTERVAL
no ip igmp query-interval
```

INTERVAL <1-18000> Frequency (in seconds) at which IGMP host query messages are sent. Default: 125 seconds.

4. Example:

The following example changes the frequency of sending IGMP host-query messages to 2 minutes on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp query-interval 120
switch_a(config-if)#
```

IGMP querier:

Max-response-time:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp query-max-response-time command to configure the maximum response time advertised in IGMP queries.

To restore to the default value, use the no ip igmp query-max-response-time command.

3. Command Syntax:

```
ip igmp query-max-response-time RESPONSETIME
no ip igmp query-max-response-time
```

RESPONSETIME <1-240> Maximum response time (in seconds) advertised in IGMP queries. Default: 10 seconds.

4. Example:

The following example configures a maximum response time of 8 seconds on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp query-max-response-time 8
switch_a(config-if)#
```

IGMP passive snooping:

Static mc router port:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp snooping mrouter interface command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the no ip igmp snooping mrouter interface command to remove the static configuration of the interface as a multicast router interface.

3. Command Syntax:

(no) ip igmp snooping mrouter interface IFNAME

IFNAME Specify the name of the interface

4. Example:

The following example shows interface fe1 (port 1) statically configured to be a multicast router interface on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping mrouter interface fe1
switch_a(config-if)#
```

IGMP passive snooping:

Report suppression:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use ip igmp snooping report-suppression command to enable report suppression for IGMP versions 1 and 2.

Use the no ip igmp snooping report-suppression command to disable report suppression.

3. Command Syntax:

(no) ip igmp snooping report-suppression

4. Example:

The following example enables report suppression for IGMPv2 reports on vlan1.1:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 2
switch_a(config-if)#ip igmp snooping report-suppression
switch_a(config-if)#
```

Force Forwarding Port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to force forward multicast packet to interface before the interface receiving IGMP query.

3. Command Syntax:

ip igmp snooping force-forward LINE none all

LINE Interface name list, ex: fe1-fe3, fe5.

none Not forward multicast packet to any interface.

all Forward multicast packet to all interfaces.

4. Example:

The following example force forwards multicast packet to interfaces fe1-fe3 and fe5:

```
switch_a(config)# ip igmp snooping force-forward fe1-fe3, fe5
switch_a(config)#
```

Passive Mode Forwarding Port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to forward multicast packet to interface before the interface receiving IGMP query in passive mode.

3. Command Syntax:

ip igmp snooping passive-forward LINE none all

LINE Interface name list, ex: fe1-fe3, fe5.

none Not forward multicast packet to any interface.

all Forward multicast packet to all interfaces.

4. Example:

The following example forwards multicast packet to interfaces fe1-fe3 and fe5:

```
switch_a(config)# ip igmp snooping passive-forward fe1-fe3, fe5
switch_a(config)#
```

NTP

RTC Time:

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The switch_a> or switch_a# prompt will show on the screen.

```
switch_a>
switch_a#
```

2. Usage:

Use the show rtc time command to show RTC time.

3. Command Syntax:

```
show rtc time
```

4. Example:

The following example shows the use of show rtc time to show RTC time:

```
switch_a>show rtc time
```

Adjust RTC Time:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use this command to configure the time of RTC.

3. Command Syntax:

```
set clock YEAR MONTH DAY HOUR MINUTE SECOND
 YEAR Specifies year from 2000 to 2037.
 MONTH <1-12> Specifies from 1 to 12.
 DAY <1-31> Specifies from 1 to 31.
 HOUR <0-23> Specifies from 0 to 23.
 MINUTE <0-59> Specifies from 0 to 59.
 SECOND <0-59> Specifies from 0 to 59.
```

4. Example:

The following example sets the time of RTC as July/20/2015 12:30:50:

```
switch_a#set clock 2015 7 20 12 30 50
switch_a#
```

NTP Status:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use ntp enable command to enable NTP for the Switch.

Use no ntp enable command to disable NTP for the Switch.

3. Command Syntax:

```
(no) ntp enable
```

4. Example:

The following example enables NTP for the Switch:

```
switch_a(config)#ntp enable
switch_a(config)#
```

NTP Server:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use this command to specify the IP address or Domain name of NTP server.

3. Command Syntax:

ntp server IP-ADDRESS | DOMAIN-NAME

IP-ADDRESS A.B.C.D specifies the IP address of NTP server.

DOMAIN-NAME Specifies the Domain name of NTP server.

4. Example:

The following example specifies the IP address (192.168.1.100) of NTP server:

```
switch_a(config)#ntp server 192.168.1.100
switch_a(config)#
```

Sync Time:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

switch_a(config)#

2. Usage:

Use ntp sync-time command to synchronize time with NTP server.

3. Command Syntax:

ntp sync-time

4. Example:

The following example synchronizes time with NTP server:

```
switch_a(config)#ntp sync-time
switch_a(config)#
```

Time Zone:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to to set time zone.

3. Command Syntax:

```
clock timezone TIMEZONE
```

TIMEZONE Specifies the time zone. (Please refer the Appendix B)

4. Example:

The following example sets time zone (Canada/Yukon):

```
switch_a(config)#clock timezone YST9YDT
switch_a(config)#
```

Polling Interval:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the polling interval.

3. Command Syntax:

```
ntp polling-interval MINUTE
```

MINUTE <1-10080> The polling interval. Enter a value in the range 1 to 10080 minutes.

4. Example:

The following example specifies the polling interval 60 minutes:

```
switch_a(config)#ntp polling interval 60
switch_a(config)#
```

Daylight Saving Mode:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable daylight saving.

Use no clock summer-time command to disable daylight saving.

3. Command Syntax:

clock summer-time TIMEZONE weekday WEEK DAY MONTH HOUR MINUTE WEEK DAY MONTH HOUR MINUTE OFFSET

TIMEZONE Specifies the daylight saving timezone.

WEEK <1-5> Specifies starting/ending week of daylight savings time.

DAY <0-6> Specifies from Sunday to Saturday.

MONTH <1-12> Specifies from January to December.

HOUR <0-23> Specifies from 0 to 23.

MINUTE <0-59> Specifies from 0 to 59.

OFFSET <1-1440> Specifies from 1 to 1440 minutes.

clock summer-time TIMEZONE date DAY MONTH HOUR MINUTE DAY MONTH HOUR MINUTE OFFSET

TIMEZONE Specifies the daylight saving timezone.

DAY <1-31> Specifies from 1 to 31.

MONTH <1-12> Specifies from January to December.

HOUR <0-23> Specifies from 0 to 23.

MINUTE <0-59> Specifies from 0 to 59.

OFFSET <1-1440> Specifies from 1 to 1440 minutes.

no clock summer-time

4. Example:

The following example sets clock summer-time TIMEZONE (onehour) as daylight saving offset 60 minutes from 4 April AM0:00 to 31 October AM0:00:

```
switch_a(config)#clock summer-time onehour date 4 4 0 0 31 10 0 0 60
switch_a(config)#
```

GMRP

Clear GMRP Statistics:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use this command to clear GMRP statistics for a given VLAN or all the VLANs configured on the Layer-2 switch. This default clearing is for all the configured VLANs.

3. Command Syntax:

clear gmrp statistics [all | vlanid VLANID] bridge BRIDGE_NAME

all Clear GMRP statistics for all the VLANs.

VLANID vlanid <1 to 4094> Clear GMRP statistics for the particular VLAN ID.

BRIDGE_NAME Bridge instance name.

4. Example:

The following example clears the GMRP statistics for VLAN 12 on bridge 1:

```
switch_a#clear gmrp statistics vlanid 12 bridge 1
switch_a#
```

The following example clears the GMRP statistics for all the configured VLANs on bridge 1:

```
switch_a#clear gmrp statistics all bridge 1
switch_a#
```

Set GMRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable/disable GMRP globally on a particular bridge. This command does not enable/disable GMRP in all ports of the bridge. After enabling GMRP globally, use the set port gmrp command to enable GMRP on individual ports of the bridge. GMRP cannot be enabled if IGMP Snooping is enabled, or if GMRP has already been configured for a particular VLAN.

3. Command Syntax:

set gmrp enable | disable bridge BRIDGE_NAME

enable Enable GMRP on Layer-2 switch.

disable Disable GMRP on Layer-2 switch

BRIDGE_NAME The text string to use for the name of the bridge.

4. Example:

The following example enables GMRP on a Layer-2 switch for bridge 1:

```
switch_a(config)#set gmrp enable bridge 1
switch_a(config)#
```

Set Port GMRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable/disable GMRP on a particular port in all VLANs or all ports in a bridge. GMRP on a port cannot be enabled for all VLANs if GMRP has already been configured for a particular VLAN for the port.

3. Command Syntax:

```
set port gmrp enable | disable all | IF_NAME
```

enable Enable GMRP on Layer-2 switch port

disable Disable GMRP on Layer-2 switch port

all All ports added to recently configured bridge

IF_NAME Specify the name of the interface.

4. Example:

The following example enables GMRP on interface fe1 (port 1):

```
switch_a(config)#set port gmrp enable fe1
switch_a(config)#
```

The following example enables GMRP on all ports:

```
switch_a(config)#set port gmrp enable all
switch_a(config)#
```

GMRP Registration:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set GMRP registration type for all ports for a given bridge.

3. Command Syntax:

```
set gmrp registration normal | fixed | forbidden IF_NAME
```

normal Specify dynamic GMRP multicast registration and deregistration on the port.

fixed Specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.

forbidden Specify that all GMRP multicasts are deregistered, and prevent any further GMRP multicast registration on the port.

IF_NAME Defines a text string used as the name of the interface; ASCII string from 1 to 16 characters.

4. Example:

The following example sets interface fe1 (port 1) to normal registration:

```
switch_a(config)#set gmrp registration normal fe1
switch_a(config)#
```

GMRP Forward All:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the GMRP forward all option for an interface.

3. Command Syntax:

```
set gmrp fwdall enable | disable IF_NAME
```

IF_NAME Interface name.

4. Example:

The following example enables GMRP forwarding on a Layer-2 switch for interface fe1 (port 1):

```
switch_a(config)#set gmrp fwdall enable fe1
switch_a(config)#
```

Set GMRP Timer:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the values for the GMRP Join, Leave, and Leaveall timers for a specified bridge. The default is the join timer (200 milliseconds); the leave timer is 600 milliseconds (ms); and the leaveall timer is 10000 milliseconds (ms).

3. Command Syntax:

```
set gmrp timer [join | leave | leaveall] TIMER_VALUE IF_NAME
```

join Type of timer

leave Type of timer

leaveall Type of timer

TIMER_VALUE Timervalue in centiseconds.

IF_NAME Specify the name of the interface.

4. Example:

The following example sets the join timers 100 centiseconds for interface fe1 (port 1):

```
switch_a(config)#set gmrp join timer 100 fe1
switch_a(config)#
```

DHCP Server

DHCP Binding Table:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The switch_a# prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use show dhcp-server binding command to display DHCP Server information.

3. Command Syntax:

show dhcp-server binding

4. Example:

The following example displays DHCP Server information:

```
switch_a#show dhcp-server binding
```

DHCP Server Status:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).

Then logon to Interface mode.

vlan1.1 means vlan 1.

The switch_a(config-if)# prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:

Use dhcp-server enable command to start the DHCP Server.

Use no dhcp-server enable command to disable DHCP Server.

3. Command Syntax:

(no) dhcp-server enable

4. Example:

The following example starts the DHCP Server:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#dhcp-server enable
switch_a(config-if)#
```

DHCP Server Range:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default IP lease block for the DHCP Server.

3. Command Syntax:

dhcp-server range A.B.C.D A.B.C.D

A.B.C.D The default Start IP for the DHCP Server.

A.B.C.D The default End IP for the DHCP Server.

4. Example:

The following example sets the default IP lease block for the DHCP Server:

```
switch_a(config)#dhcp-server range 192.168.1.100 192.168.1.250
switch_a(config)#
```

DHCP Server Subnet-mask:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default subnet mask for the DHCP Server.

Use the no form of this command to remove this setting.

3. Command Syntax:

```
dhcp-server subnet-mask A.B.C.D
no dhcp-server subnet-mask
```

A.B.C.D The default subnet mask for the DHCP Server.

4. Example:

The following example sets the default subnet mask for the DHCP Server:

```
switch_a(config)#dhcp-server subnet-mask 255.255.255.0
switch_a(config)#
```

DHCP Server Gateway:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default gateway for the DHCP Server.

Use the no form of this command to remove this setting.

3. Command Syntax:

```
dhcp-server gateway A.B.C.D
no dhcp-server gateway
```

A.B.C.D The default gateway for the DHCP Server.

4. Example:

The following example sets the default gateway for the DHCP Server:

```
switch_a(config)#dhcp-server gateway 192.168.1.254
switch_a(config)#
```

DHCP Server DNS:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default DNS for the DHCP Server.

Use the no form of this command to remove this setting.

3. Command Syntax:

```
dhcp-server dns 1 | 2 A.B.C.D
no dhcp-server dns 1 | 2
```

A.B.C.D The default DNS for the DHCP Server.

4. Example:

The following example sets the default DNS for the DHCP Server:

```
switch_a(config)#dhcp-server dns 1 192.168.1.20
switch_a(config)#
```

DHCP Server Lease Time:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The switch_a(config)# prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default lease time for the DHCP Server. Use the value 0 to reset this setting.

3. Command Syntax:

```
dhcp-server lease-time <0-86400>
```

<0–86400> The default lease time for the DHCP Server (default: 86400).

4. Example:

The following example sets the default lease time for the DHCP Server:

```
switch_a(config)#dhcp-server lease-time 86400
switch_a(config)#
```

Appendix A. DB9 DCE Pin Assignment.

Pin Number	Name	RS-232 Signal Name
1	DCD	Data Carrier Detect
2	RxD	Received Data
3	TxD	Transmit Data
4	—	Not connected
5	GND	Signal Ground
6	DSR	Data Set Ready
7	—	Not connected
8	CTS	Clear to Send
9	—	Not connected

Appendix B. Time Zones

Time Zone	Country and City Lists
Europe	
MEZ-1MESZ	Europe/Vienna, Europe/Berlin, Europe/Zurich
MET-1METDST	Africa/Tunis, CET, MET, Europe/Tirane, Europe/Andorra, Europe/Brussels, Europe/Prague, Europe/Copenhagen, Europe/Paris, Europe/Gibraltar, Europe/Budapest, Europe/Rome, Europe/Vaduz, Europe/Luxembourg, Europe/Malta, Europe/Monaco, Europe/Amsterdam, Europe/Oslo, Europe/Warsaw, Europe/Belgrade, Europe/Madrid, Africa/Ceuta, Europe/Stockholm, Europe/Vatican, Europe/San_Marino, Arctic/Longyearbyen, Atlantic/Jan_Mayen, Europe/Ljubljana, Europe/Sarajevo, Europe/Skopje, Europe/Zagreb, Europe/Bratislava, Poland
EET-2EETDST	Asia/Nicosia, EET, Europe/Minsk, Europe/Sofia, Europe/Athens, Europe/Vilnius, Europe/Chisinau, Europe/Istanbul, Europe/Kiev, Europe/Uzhgorod, Europe/Zaporozhye, Europe/Nicosia, Asia/Istanbul, Europe/Tiraspol, Turkey
GMT0BST	Europe/London, Europe/Dublin, Eire, Europe/Belfast, GB, GB-Eire
WET0WETDST	WET, Atlantic/Faeroe, Atlantic/Madeira, Atlantic/Canary
PWT0PST	Europe/Lisbon, Portugal
MST-3MDT	Europe/Moscow, W-SU
EUT-1EUTDST	America/Scoresbysund, Atlantic/Azores
EUT-2EUTDST	Asia/Beirut, Europe/Simferopol
EUT-3EUTDST	Asia/Tbilisi
EUT-4EUTDST	Europe/Samara
EUT-6EUTDST	Asia/Almaty, Asia/Qyzylorda
EUT-8EUTDST	Asia/Ulaanbaatar
Russian Federation	
RFT-2RFTDST	Europe/Kaliningrad
RFT-3RFTDST	Europe/Moscow
RFT-4RFTDST	Asia/Yerevan, Asia/Baku, Asia/Oral, Asia/Ashkhabad
RFT-5RFTDST	Asia/Aqtobe, Asia/Aqtau, Asia/Bishkek, Asia/Yekaterinburg
RFT-6RFTDST	Asia/Omsk, Asia/Novosibirsk
RFT-7RFTDST	Asia/Hovd, Asia/Krasnoyarsk
RFT-8RFTDST	Asia/Irkutsk, Asia/Chungking, Asia/Ulan_Bator
RFT-9RFTDST	Asia/Choibalsan, Asia/Yakutsk
RFT-10RFTDST	Asia/Vladivostok
RFT-11RFTDST	Asia/Sakhalin, Asia/Magadan
RFT-12RFTDST	Asia/Kamchatka, Asia/Anadyr

Time Zone	Country and City Lists
North America	
PST8PDT	America/Los_Angeles, US/Pacific-New, PST8PDT, US/Pacific, SystemV/PST8PDT
MST7MDT	America/Denver, America/Boise, America/Cambridge_Bay, America/Shiprock, MST7MDT, Navajo, US/Mountain, SystemV/MST7MDT
MST7	America/Phoenix, MST, US/Arizona, SystemV/MST7
CST6CDT	America/Chicago, America/North_Dakota/Center, America/Menominee, America/Costa_Rica, America/Managua, CST6CDT, US/Central, SystemV/CST6CDT
EST5EDT	America/New_York, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Detroit, America/Pangnirtung, America/Louisville, EST5EDT, US/Eastern, US/Michigan, SystemV/EST5EDT
AST4ADT	America/Thule, Atlantic/Bermuda, SystemV/AST4ADT
EST5	America/Coral_Harbour, America/Cayman, America/Jamaica, America/Panama, EST, Jamaica, SystemV/EST5
AST10ADT	America/Adak, America/Atka, US/Aleutian
YST9YDT	Canada/Yukon
NST3:30NDT	America/St_Johns, Canada/Newfoundland
NAST3NADT	America/Godthab, America/Miquelon
NAST9NADT	Pacific/Pitcairn, America/Juneau, America/Yakutat, America/Anchorage, America/Nome, US/Alaska, SystemV/YST9YDT, SystemV/PST8
South America and Central America	
TTST4	America/Port_of_Spain
SAT3	America/Argentina/Buenos_Aires, America/Argentina/Cordoba, America/Argentina/Tucuman, America/Argentina/La_Rioja, America/Argentina/San_Juan, America/Argentina/Jujuy, America/Argentina/Catamarca, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Ushuaia, America/Argentina/ComodRivadavia, America/Buenos_Aires, America/Cordoba, America/Jujuy, America/Mendoza
EBST3EBDT	America/Fortaleza, America/Recife, America/Araguaina, America/Maceio, America/Bahia, America/Sao_Paulo, America/Cuiaba, America/Montevideo, America/Catamarca, America/Rosario, Brazil/East
WBST4WBDT	America/Campo_Grande, America/Boa_Vista, America/Manaus, Atlantic/Stanley, America/Asuncion, Brazil/West
ACRE5	America/Rio_Branco, America/Porto_Acre, Brazil/Acre
NORO2	America/Noronha, Brazil/DeNoronha
CST4CDT	Antarctica/Palmer, America/Santiago, Chile/Continental
EIST6EIDT	Pacific/Easter, Chile/EasterIsland
Asia	
MST-8	Asia/Kuala_Lumpur, Asia/Kuching
CST-8	Asia/Harbin, Asia/Shanghai, Asia/Chongqing, Asia/Urumqi, Asia/Kashgar, Asia/Hong_Kong, Asia/Macau, Asia/Macao, Hongkong, PRC, ROC

=

Time Zone	Country and City Lists
Oceania	
CST-9:30CDT	Australia/Adelaide, Australia/Broken_Hill, Australia/South, Australia/Yancowinna
EST-10EDT	Australia/Brisbane, Australia/Lindeman, Australia/Currie, Australia/Melbourne, Australia/Sydney, Australia/ACT, Australia/Canberra, Australia/NSW, Australia/Queensland, Australia/Tasmania, Australia/Victoria
LHT-10:30LHDT	Australia/Lord_Howe, Australia/LHI
TST-10TDT	Australia/Hobart
NZST-12NZDT	Antarctica/McMurdo, Pacific/Auckland, Antarctica/South_Pole, NZ
CIST-12:45CIDT	Pacific/Chatham, NZ-CHAT
Africa	
SAST-2	Africa/Maseru, Africa/Johannesburg, Africa/Mbabane
EST-2EDT	Africa/Cairo, Egypt
UAEST-4	Asia/Dubai
IST-3IDT	Asia/Baghdad
JST-2JDT	Asia/Amman
SST-2SDT	Asia/Damascus
Universal	
UCT	Africa/Ouagadougou, Africa/Abidjan, Africa/Banjul, Africa/Accra, Africa/Conakry, Africa/Bissau, Africa/Monrovia, Africa/Bamako, Africa/Nouakchott, Africa/Casablanca, Africa/El_Aaiun, Atlantic/St_Helena, Africa/Sao_Tome, Africa/Dakar, Africa/Freetown, Africa/Lome, America/Danmarkshavn, Atlantic/Reykjavik, Etc/GMT, Etc/UTC, Etc/UCT, GMT, Etc/Universal, Etc/Zulu, Etc/Greenwich, Etc/GMT-0, Etc/GMT+0, Etc/GMT0, Africa/Timbuktu, GMT+0, GMT-0, GMT0, Greenwich, Iceland, UCT, UTC, Universal, Zulu
UCT1	Atlantic/Cape_Verde, Etc/GMT+1
UCT2	Atlantic/South_Georgia, Etc/GMT+2
UCT3	Antarctica/Rothera, America/Belem, America/Cayenne, America/Paramaribo, Etc/GMT+3
UCT4	America/Anguilla, America/Antigua, America/Barbados, America/Dominica, America/Grenada, America/Guadeloupe, America/Martinique, America/Montserrat, America/Puerto_Rico, America/St_Kitts, America/St_Lucia, America/St_Vincent, America/Tortola, America/St_Thomas, America/Aruba, America/La_Paz, America/Porto_Velho, America/Curacao, America/Caracas, America/Guyana, Etc/GMT+4, America/Virgin, SystemV/AST4
UCT5	America/Guayaquil, America/Eirunepe, America/Lima, Etc/GMT+5
UCT6	America/Belize, America/El_Salvador, America/Tegucigalpa, Pacific/Galapagos, Etc/GMT+6
UCT7	Etc/GMT+7
UCT8	Etc/GMT+8
UCT9	Pacific/Gambier, Etc/GMT+9, SystemV/YST9
UCT10	Pacific/Rarotonga, Pacific/Tahiti, Pacific/Fakaofo, Pacific/Johnston, Pacific/Honolulu, Etc/GMT+10, HST, US/Hawaii, SystemV/HST10

Time Zone	Country and City Lists
Universal (continued from previous page)	
UCT11	Pacific/Niue, Pacific/Pago_Pago, Pacific/Apia, Pacific/Midway, Etc/GMT+11, Pacific/Samoa, US/Samoa
UCT-1	Africa/Algiers, Africa/Luanda, Africa/Porto-Novo, Africa/Douala, Africa/Bangui, Africa/Ndjamena, Africa/Kinshasa, Africa/Brazzaville, Africa/Malabo, Africa/Libreville, Africa/Windhoek, Africa/Niamey, Africa/Lagos, Etc/GMT-1
UCT-2	Africa/Gaborone, Africa/Bujumbura, Africa/Lubumbashi, Africa/Tripoli, Africa/Blantyre, Africa/Maputo, Africa/Kigali, Africa/Lusaka, Africa/Harare, Etc/GMT-2, Libya
UCT-3	Indian/Comoro, Africa/Djibouti, Africa/Asmera, Africa/Addis_Ababa, Africa/Nairobi, Indian/Antananarivo, Indian/Mayotte, Africa/Mogadishu, Africa/Khartoum, Africa/Dar_es_Salaam, Africa/Kampala, Antarctica/Syowa, Asia/Bahrain, Asia/Kuwait, Asia/Qatar, Asia/Riyadh, Asia/Aden, Etc/GMT-3
UCT-4	Indian/Mauritius, Indian/Reunion, Indian/Mahe, Asia/Muscat, Etc/GMT-4
UCT-5	Indian/Kerguelen, Indian/Maldives, Asia/Karachi, Asia/Dushanbe, Asia/Ashgabat, Asia/Samarkand, Asia/Tashkent, Etc/GMT-5
UCT-5:45	Asia/Katmandu
UCT-6	Antarctica/Mawson, Antarctica/Vostok, Asia/Dhaka, Asia/Thimphu, Indian/Chagos, Asia/Colombo, Etc/GMT-6, Asia/Dacca, Asia/Thimbu
UCT-6:30	Asia/Rangoon, Indian/Cocos
UCT-7	Antarctica/Davis, Asia/Phnom_Penh, Asia/Jakarta, Asia/Pontianak, Asia/Vientiane, Asia/Bangkok, Asia/Saigon, Indian/Christmas, Etc/GMT-7
UCT-8	Antarctica/Casey, Asia/Brunei, Asia/Taipei, Asia/Makassar, Asia/Manila, Asia/Singapore, Etc/GMT-8, Asia/Ujung_Pandang, Singapore
UCT-9	Asia/Dili, Asia/Jayapura, Pacific/Palau, Etc/GMT-9
UCT-9:30	Australia/Darwin, Australia/North
UCT-10	Antarctica/DumontDUrville, Pacific/Guam, Pacific/Saipan, Pacific/Truk, Pacific/Noumea, Pacific/Port_Moresby, Etc/GMT-10, Pacific/Yap
UCT-11	Pacific/Ponape, Pacific/Kosrae, Pacific/Guadalcanal, Etc/GMT-11
UCT-11:30	Pacific/Norfolk
UCT-12	Pacific/Fiji, Pacific/Tarawa, Pacific/Enderbury, Pacific/Majuro, Pacific/Kwajalein, Pacific/Nauru, Pacific/Tongatapu, Pacific/Funafuti, Pacific/Wake, Pacific/Efate, Pacific/Wallis, Etc/GMT-12, Kwajalein
UCT-13	Etc/GMT-13
JST	Asia/Tokyo, Japan
KST	Asia/Seoul, Asia/Pyongyang, ROK
UCT-3:30	Asia/Tehran, Iran
UCT-4:30	Asia/Kabul
IST-2IDT	Asia/Jerusalem, Asia/Gaza, Asia/Tel_Aviv, Israel
CST6MEX	America/Cancun, America/Merida, America/Monterrey, America/Mexico_City, America/Lima, Mexico/General

Time Zone	Country and City Lists
Universal (continued from previous page)	
CST6	America/Regina, America/Swift_Current, Canada/East-Saskatchewan, Canada/Saskatchewan, SystemV/CST6
EET-2EETDST2	Europe/Bucharest
EET-2EETDST3	Europe/Tallinn, Europe/Helsinki, Europe/Riga, Europe/Mariehamn
EET-2EETDST2W2K	Europe/Istanbul
UCT-14	Pacific/Kiritimati, Etc/GMT-14
UCT9:30	Pacific/Marquesas
UCT12	Etc/GMT+12
North America (Canada)	
PST8PDT_CA	America/Vancouver, America/Dawson_Creek, America/Whitehorse, America/Dawson, Canada/Pacific
MST7MDT_CA	America/Edmonton, America/Yellowknife, America/Inuvik, Canada/Mountain
CST6CDT_CA	America/Rainy_River, America/Winnipeg, America/Rankin_Inlet, Canada/Central
EST5EDT_CA	America/Montreal, America/Toronto, America/Thunder_Bay, America/Nipigon, America/Iqaluit, Canada/Eastern
AST4ADT_CA	America/Goose_Bay, America/Halifax, America/Glace_Bay, Canada/Atlantic
North America (Cuba)	
EST5EDT_CU	America/Havana, Cuba
North America (Haiti)	
EST5EDT_HT	America/Nassau, America/Santo_Domingo, America/Port-au-Prince, America/Bogota
North America (Mexico)	
PST8PDT_MX	America/Tijuana, America/Ensenada, Mexico/BajaNorte
MST7MDT_MX	America/Chihuahua, America/Hermosillo, America/Mazatlan, Mexico/BajaSur
CST6CDT_MX	America/Guatemala
North America (Turks and Caicos)	
EST5EDT_TC	America/Grand_Turk
Additions Since 10g RTM	
EST5EDT_INDIANA	America/Indiana/Indianapolis, America/Indiana/Marengo, America/Indiana/Vevay, America/Fort_Wayne, America/Indianapolis, America/Indiana/Knox, America/Knox_IN, US/Indiana-Starke, US/East-Indiana
UCT-8_WA	Australia/Perth, Australia/West

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.

Great tech support is just 60 seconds away at 724-746-5500 or blackbox.com.

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 60 seconds or less.

© Copyright 2014. Black Box Corporation. All rights reserved. Black Box® and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Any third-party trademarks appearing in this manual are acknowledged to be the property of their respective owners.

LEH908A User Manual, version 3